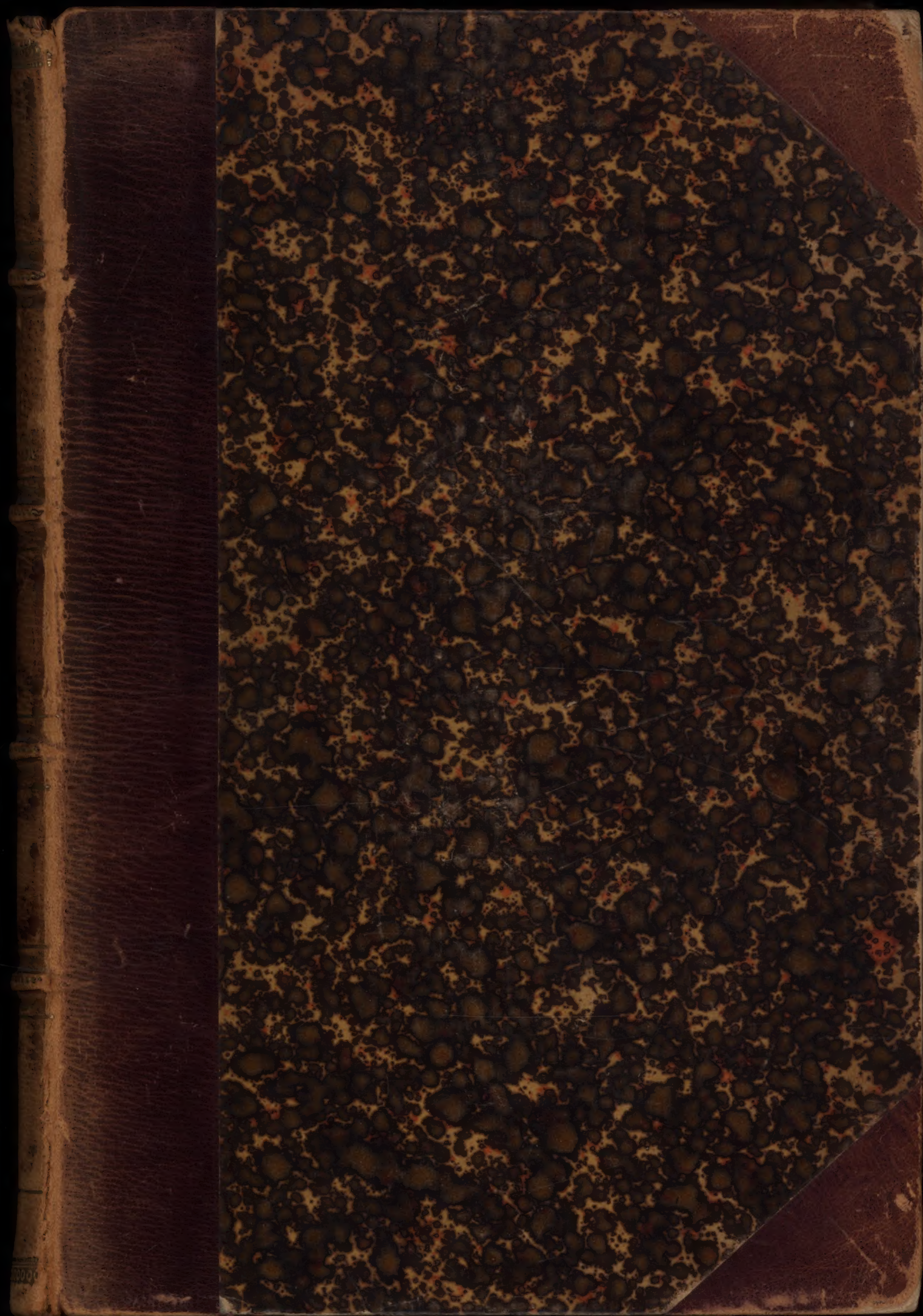
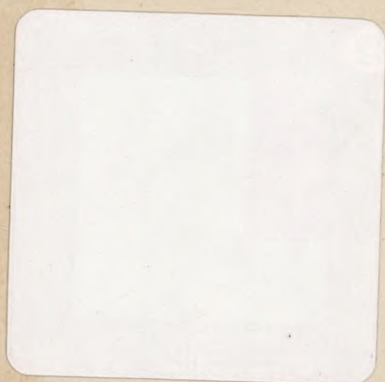






Weidmannsche Buchhandlung Berlin. Gravure Meisenbach Riffarth & Co. Berlin.

C. F. GAUSS.

26 [illegible]

Carl Friedrich Gauss'

Untersuchungen über höhere Arithmetik.

(Disquisitiones arithmeticae. Theorematis arithmetici demonstratio nova. Summatio quarumdam serierum singularium. Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae. Theoria residuorum biquadraticorum, commentatio prima et secunda. Etc.)

Deutsch herausgegeben

von

H. Maser.



Berlin.

Verlag von Julius Springer.

1889.

Vorwort des Herausgebers.

Das Studium der herrlichen Geisteserzeugnisse unseres unsterblichen Gauss ist für jeden Mathematiker, der es ernsthaft mit seiner Wissenschaft meint, eine unabweisbare Pflicht. Grossen Dank ist man daher der Königlichen Gesellschaft der Wissenschaften zu Göttingen schuldig, dass sie durch Veranstaltung einer billigen in einzelnen Bänden erhältlichen Ausgabe der Gauss'schen Werke im Originaltext jedermann in den Stand gesetzt hat, sich dieselben anzuschaffen. Wenn nun trotz der leichten Erhältlichkeit des Originals hier noch der Versuch mit einer deutschen Ausgabe der *Disquisitiones arithmeticae* und der in lateinischer Sprache geschriebenen im zweiten Bande der Gesammelten Werke enthaltenen zahlentheoretischen Abhandlungen gewagt wird, so hat dies in der Erwägung seinen Grund, dass eben die sprachlichen Schwierigkeiten des Originals für viele Leser keine geringen sind und um so drückender empfunden werden, als das Verständnis des Inhaltes selbst, und zwar nicht bloss beim ersten Studium desselben, eine sehr bedeutende Geistesthätigkeit erfordert und alle Kräfte in Anspruch nimmt. Der des Faches kundige Gelehrte wird allerdings lieber zum Originale greifen. Denn wie in den Augen des Kenners ein Werk der Skulptur oder Malerei zwar durch die Gediegenheit und Bedeutung des behandelten Stoffes und durch die Feinheit in der Anordnung und Ausführung der einzelnen Teile Anerkennung findet, aber erst durch die Thatsache, dass es Original ist, seinen wahren Wert erhält, so auch ein Werk der schöngeistigen oder fachwissenschaftlichen Literatur. Nur das Originalwerk zeigt uns die Genialität seines Schöpfers im vollen Glanze und erfüllt uns mit jenem geistigen Vergnügen, welches die Bewunderung grosser Männer gewährt. Da nun die *Disquisitiones arithmeticae* ein durch seinen Inhalt wie durch seine Form hervorragendes klassisches Werk sind, so kann das Studium derselben im Originaltext nicht dringend genug empfohlen werden. Wem es aber zunächst nur darum zu thun ist, mit dem Inhalte selbst bekannt zu werden, der wird es jedenfalls dankbar annehmen, wenn es ihm durch Hinwegräumung äusserer Schwierigkeiten ermöglicht wird, seine ganze Aufmerksamkeit auf die Sache zu richten. Daher darf man sich immerhin der Hoffnung hingeben, dass die vorliegende deutsche Ausgabe vielen Lesern sehr willkommen sein wird.

Was nun diese Ausgabe selbst anlangt, so hätten in dieselbe von den kleineren Abhandlungen wohl nur die von Gauss selbst veröffentlichten aufgenommen werden sollen; ich habe aber auch die in seinem Nachlasse vorgefundenen, im zweiten Bande seiner Werke enthaltenen Fragmente nicht ausschliessen wollen, weil sie noch manches Goldkörnchen, manche wertvolle Bemerkungen und interessante Sätze enthalten, obwohl sie weder sachlich noch formell vollkommen druckfertig genannt werden können und daher wohl in der Gesamtausgabe seiner Werke aber nicht hier einen Platz beanspruchen durften. Um den Character und Geist der Gauss'schen Arbeiten möglichst rein und frei von jedem Beiwerk wiederzuspiegeln, habe ich mich aller eigenen Anmerkungen enthalten und nur die bereits sanctionierten, von Herrn Professor Dedekind herrührenden Bemerkungen zu einigen Abhandlungen mit gütiger Erlaubnis des Verfassers aus dem zweiten Bande der Göttinger Ausgabe übernommen.

Für diejenigen, denen dieser Band selbst nicht zur Hand ist, füge ich zur Orientierung hier noch einige daraus entnommene Notizen hinzu. An einigen Stellen der *Disqu. arithm.* wird auf einen achten Abschnitt verwiesen, obwohl ein solcher nicht vorhanden ist; ferner haben die hier mitgeteilten Artikel aus der „Lehre von den Resten" und die Abhandlung auf Seite 678 eine eigentümliche Numerierung. Es findet dies dadurch seine Erklärung, dass Gauss seine ursprünglichen Aufzeichnungen, welche den Titel *„Analysis residuorum"* tragen, einer gänzlichen Umarbeitung unterzog, aus welcher die *Disquisitiones arithmeticae* hervorgingen, deren achter Abschnitt die auf Seite 589 u. ff. mitgeteilten Untersuchungen zum Gegenstande haben sollte. Als zu umfangreich wurden diese Untersuchungen aber schliesslich von den *Disqu. arithm.* ausgeschlossen und der achte Abschnitt einer eingehenderen Betrachtung der Lehre von der Kreisteilung vorbehalten, daher das darauf bezügliche Fragment (Seite 678) sich in der Numerierung seiner Artikel unmittelbar an die *Disqu. arithm.* anschliesst. Die Artikel in den beiden Abschnitten aus der „Lehre von den Resten" tragen dieselben Nummern wie im ursprünglichen Manuskript.

Vor einigen Jahren ist von mir eine Übersetzung des so überaus selten gewordenen Legendre'schen Werkes *„Théorie des nombres"* herausgegeben worden; es sei mir erlaubt, meiner Freude darüber Ausdruck zu geben, dass es mir vergönnt war, auch das zweite und bedeutendere klassische Werk über Zahlentheorie, die *Disquisitiones arithmeticae* von Gauss, dem mathematischen Publikum in deutscher Sprache zu überreichen. Ich hoffe damit der Wissenschaft auch einen kleinen Dienst erwiesen zu haben.

Berlin, im März 1889.

Der Herausgeber.

Vorrede des Verfassers zu den Arithmetischen Untersuchungen.

Die in diesem Werke enthaltenen Untersuchungen beziehen sich auf denjenigen Teil der Mathematik, der es mit den ganzen Zahlen zu thun hat, während die gebrochenen Zahlen meistenteils, die ~~imaginären~~ irrationalen immer ausgeschlossen bleiben. Die sogenannte unbestimmte oder Diophantische Analysis, welche aus unendlich vielen dem unbestimmten Problem genügenden Lösungen diejenigen auszuwählen lehrt, welche ganzzahlig oder wenigstens rational sind (meistens auch noch unter der Bedingung, dass sie positiv seien), ist nicht jene Disziplin selbst, sondern vielmehr ein sehr specieller Teil derselben und verhält sich zu ihr ungefähr so, wie die Kunst, die Gleichungen zu reduzieren und aufzulösen (Algebra), zur gesamten Analysis. Wie nämlich in das Gebiet der Analysis alle Untersuchungen gehören, welche über die allgemeinen Eigenschaften und Beziehungen der Zahlgrössen angestellt werden können, so bilden die ganzen Zahlen (und die gebrochenen, insofern sie durch ganze bestimmt werden) den eigentlichen Gegenstand der Arithmetik. Da aber das, was gewöhnlich unter dem Namen Arithmetik gelehrt wird, kaum über die Kunst zu zählen und zu rechnen (d. h. die Zahlen durch geeignete Zeichen etwa nach dem dekadischen Systeme darzustellen und die arithmetischen Operationen auszuführen) hinausgeht, mit Hinzufügung noch einiger Sachen, die entweder gar nicht zur Arithmetik gehören (wie die Lehre von den Logarithmen) oder doch wenigstens nicht den ganzen Zahlen eigentümlich sind, sondern für alle Zahlgrössen gelten, so scheint es sachgemäss zu sein, zwei Teile der Arithmetik zu unterscheiden und das Erwähnte zur elementaren Arithmetik zu rechnen, dagegen alle allgemeinen Untersuchungen über die eigentlichen Beziehungen der ganzen Zahlen der höheren Arithmetik, von der hier allein die Rede sein wird, zu überweisen.

Zur höheren Arithmetik gehört das, was Euclid in den „*Elementen*“ Buch VII u. ff. mit der bei den Alten gewohnten Eleganz und Strenge gelehrt hat; doch beschränkt sich dies auf die ersten Anfänge dieser Wissenschaft. Das berühmte Werk des Diophant, welches ganz den Problemen aus der unbestimmten Analysis gewidmet ist, enthält viele Unter-

suchungen, welche wegen ihrer Schwierigkeit und der Feinheit der Kunstgriffe eine nicht geringe Meinung von dem Geiste und Scharfsinn ihres Verfassers erwecken, besonders wenn man die Geringfügigkeit der Hülfsmittel bedenkt, welche ihm zu Gebote standen. Da aber diese Aufgaben mehr eine gewisse Gewandtheit und geschickte Behandlung als tiefere Prinzipien erfordern und überdies zu speciell sind und selten zu allgemeineren Schlüssen führen, so dürfte dieses Buch mehr aus dem Grunde eine Epoche in der Geschichte der Mathematik bilden, weil es die ersten Spuren einer characteristischen Kunst und der Algebra in sich enthält, als weil es die höhere Arithmetik mit neuen Entdeckungen bereichert hat. Bei weitem das Meiste verdankt man den Neueren, von denen zwar nur wenige Männer, aber Männer von unvergänglichem Ruhme, wie P. de Fermat, L. Euler, L. Lagrange, A. M. Legendre, den Zugang zu dem Heiligtume dieser göttlichen Wissenschaft erschlossen und gezeigt haben, von wie grossen Reichtümern es überfüllt ist. Ich unterlasse es jedoch hier anzuführen, welche Entdeckungen von jedem einzelnen dieser Geometer ausgegangen sind, da man dies aus den Vorreden zu den Zusätzen, mit denen Lagrange Euler's Algebra bereichert hat, und zu dem bald zu erwähnenden erst kürzlich erschienenen Werke von Legendre erfahren kann und überdies die meisten an gehöriger Stelle in diesen Arithmetischen Untersuchungen Erwähnung finden werden.

Der Zweck dieses Werkes, dessen Herausgabe ich schon vor fünf Jahren versprochen hatte, war der, die Untersuchungen aus der höheren Arithmetik, die ich teils vor teils nach jener Zeit angestellt habe, zur allgemeineren Kenntnis zu bringen. Damit sich aber Niemand wundere, dass ich die Wissenschaft hier fast von ihren ersten Anfängen an wiederholt und viele Untersuchungen von Neuem aufgenommen habe, mit denen sich schon andere beschäftigt haben, glaube ich darauf hinweisen zu müssen, dass ich, als ich mich zuerst im Anfange des Jahres 1795 dieser Art von Untersuchungen zuwandte, von allem dem, was von Neueren auf diesem Gebiete geleistet worden war, nichts wusste und aller Hülfsmittel, durch welche ich mir davon hätte einige Kenntnis verschaffen können, baar war. Während ich nämlich damals mit einer andern Arbeit beschäftigt war, stiess ich zufällig auf eine ausgezeichnete arithmetische Wahrheit (wenn ich nicht irre, war es der Satz des Artikels 108), und da ich dieselbe nicht nur an und für sich für sehr schön hielt, sondern auch vermutete, dass sie mit anderen hervorragenderen Eigenschaften im Zusammenhang stehe, bemühte ich mich mit ganzer Kraft, die Prinzipien, auf denen sie beruhte, zu durchschauen und einen strengen Beweis dafür zu erhalten. Als mir dies endlich nach Wunsch gelungen war, hatten mich die Reize dieser Untersuchungen derart

umstrickt, dass ich sie nicht mehr verlassen konnte; so kam es, dass, während das Eine immer zu dem Andern den Weg bahnte, das in den vier ersten Abschnitten dieses Werkes Mitgeteilte grösstenteils erledigt war, ehe ich von ähnlichen Arbeiten anderer Geometer etwas zu Gesicht bekommen hatte. Als mir darauf Gelegenheit wurde, die Schriften dieser grossen Geister durchzusehen, erkannte ich zwar, dass der grössere Teil meiner Überlegungen längst abgethanen Sachen gewidmet gewesen war, um so lebhafter aber bestrebte ich mich, den Fussstapfen jener folgend, die Arithmetik weiter auszubauen; so wurden verschiedene Untersuchungen angestellt, von denen die Abschnitte V, VI und VII einen Teil wiedergeben. Als ich nach einiger Zeit den Entschluss fasste, die Früchte meiner Anstrengungen zu veröffentlichen, liess ich mich, dem Wunsche vieler nachgebend, um so lieber überreden, auch von jenen früheren Untersuchungen nichts zu unterdrücken, weil es damals noch kein Buch gab, aus dem man die in den Denkschriften der Akademieen zerstreuten Arbeiten anderer Geometer über diese Gegenstände hätte kennen lernen können, sodann weil viele von ihnen vollständig neu und zum grossen Teil nach neuen Methoden behandelt waren, endlich weil sie alle sowohl unter einander als auch mit den späteren Untersuchungen durch ein so enges Band zusammenhingen, dass auch das Neue nicht bequem genug auseinandergesetzt werden konnte, ohne dass das andere von Anfang an wiederholt worden war.

Inzwischen erschien das ausgezeichnete Werk des schon vorher um die höhere Arithmetik hochverdienten Legendre, *Essai d'une théorie des nombres*, Paris a. VI, in welchem er nicht nur alles, was bis dahin in dieser Wissenschaft gearbeitet worden war, sorgfältig zusammentrug und in Ordnung brachte, sondern auch noch sehr viel Neues aus seinem Eigenen hinzuthat. Da mir dieses Buch zu spät in die Hände kam, nachdem bereits der grösste Teil meines Werkes gedruckt war, habe ich es nirgends, wo die Analogie des Gegenstandes Gelegenheit dazu gegeben hätte, erwähnen können; nur hinsichtlich einiger weniger Stellen hielt ich es für notwendig in den Zusätzen einige Bemerkungen hinzuzufügen, die der edeldenkende und aufgeklärte Mann, wie ich hoffe, nicht übeldeuten wird.

Während des Druckes dieses Werkes, welcher mehrere Male unterbrochen und durch mancherlei Hindernisse bis ins vierte Jahr hinausgezogen wurde, habe ich nicht nur diejenigen Untersuchungen, die ich zwar schon früher angefangen, deren Veröffentlichung aber ich auf eine andere Zeit zu verschieben beschlossen hatte, um nicht das Buch allzu umfangreich werden zu lassen, weiter fortgesetzt, sondern noch mehrere andere neue in Angriff genommen. Auch wurden mehrere, die ich aus demselben Grunde nur obenhin berührt habe, weil eine ausführlichere Behandlung weniger not-

wendig erschien (z. B. die, welche in den Artikeln 37, 82 u. ff. und andern Stellen angeführt sind), später wieder aufgenommen und haben dieselben zu allgemeineren Untersuchungen, die der Veröffentlichung wert erscheinen, Veranlassung gegeben (vgl. auch, was in den Zusätzen über Artikel 306 gesagt ist). Schliesslich habe ich, da das Buch besonders wegen der grossen Ausdehnung des fünften Abschnittes bei weitem umfangreicher geworden war, als ich erwartet hatte, mehreres, was anfänglich für dasselbe bestimmt war, und unter andern den ganzen achten Abschnitt (welcher in diesem Bande bereits an einigen Stellen erwähnt wird und eine allgemeine Abhandlung über die algebraischen Congruenzen jeden Grades enthält) weglassen müssen. Alles dieses, welches mit Leichtigkeit einen mit dem vorliegenden gleichstarken Band ausfüllen wird, werde ich veröffentlichen, sobald sich die Gelegenheit dazu bietet.

Dass ich bei mehreren schwierigen Untersuchungen mich synthetischer Beweise bedient und die Analysis, durch welche dieselben gefunden sind, unterdrückt habe, ist besonders durch das Streben nach Kürze veranlasst, der ich mich soviel wie möglich befleissigen musste.

Die Theorie der Kreisteilung oder der regulären Polygone, welche im siebenten Abschnitt behandelt wird, gehört zwar an und für sich nicht in die Arithmetik; doch müssen ihre Prinzipien einzig und allein aus der höheren Arithmetik geschöpft werden; dies wird vielleicht den Geometern ebenso überraschend sein, wie ihnen hoffentlich die neuen Wahrheiten, die man aus dieser Quelle schöpfen kann, angenehm sein werden.

Hierauf habe ich den Leser aufmerksam machen wollen. Über den Gegenstand selbst zu urteilen, ist nicht an mir. Ich wünsche nichts lebhafter, als dass sie denen, denen der Fortschritt der Wissenschaft am Herzen liegt, gefallen mögen, sei es nun, dass sie bisherige Lücken ausfüllen, sei es, dass sie den Zugang zu Neuem öffnen.

Inhaltsverzeichnis.

Arithmetische Untersuchungen.

Abhandlungen.

Einige Untersuchungen aus dem handschriftlichen Nachlasse von Gauss.

Arithmetische Untersuchungen.



Erster Abschnitt.

Von der Congruenz der Zahlen im Allgemeinen.

Congruente Zahlen, Moduln, Reste und Nichtreste.

1.

Wenn die Zahl a in der Differenz der Zahlen b, c aufgeht, so werden b und c nach a **congruent**, im andern Falle **incongruent** genannt. Die Zahl a nennen wir den **Modul**. Jede der beiden Zahlen b, c heisst im ersteren Falle **Rest**, im letzteren aber **Nichtrest** der andern.

Diese Bezeichnungen gelten in Bezug auf alle **ganzen**, positiven sowohl wie negativen*), Zahlen, sie sind aber nicht auf gebrochene Zahlen auszudehnen. So sind z. B. -9 und $+16$ nach dem Modul 5 congruent; -7 ist nach dem Modul 11 Rest, nach dem Modul 3 aber Nichtrest von $+15$. Da übrigens die Null durch jede beliebige Zahl geteilt wird, so ist jede Zahl als nach jedem beliebigen Modul sich selbst congruent zu betrachten.

2.

Sämtliche Reste einer gegebenen Zahl a nach dem Modul m sind in der Formel $a + km$ enthalten, wo k eine unbestimmte ganze Zahl bezeichnet. Von den Sätzen, die wir später aufstellen werden, lassen sich die leichteren hieraus ohne Mühe beweisen; doch wird jeder die Richtigkeit derselben ebenso leicht durch den blossen Anblick erkennen können.

Die Congruenz der Zahlen werden wir im Folgenden durch das Zeichen $\equiv$ andeuten und den Modul da, wo es nötig sein wird, in Klammern hinzufügen: $-16 \equiv 9$ (mod. 5), $-7 \equiv 15$ (mod. 11).**)

*) Der Modul ist offenbar stets absolut, d. h. ohne jedes Vorzeichen, zu nehmen.

**) Dieses Zeichen habe ich wegen der grossen Analogie, die zwischen der Gleichheit und der Congruenz stattfindet, gewählt. Aus demselben Grunde hat Legendre in seinem unten öfter zu erwähnenden Werke geradezu das Gleichheitszeichen für die Congruenz beibehalten; doch habe ich Bedenken getragen, ihm darin zu folgen, um keine Zweideutigkeit entstehen zu lassen.

3.

Satz. Sind m aufeinanderfolgende ganze Zahlen

$$a,\ a+1,\ a+2, \ldots, a+m-1$$

und eine andere A gegeben, so wird eine und nur eine von jenen dieser letzteren nach dem Modul m congruent sein.

Ist nämlich $\frac{a-A}{m}$ eine ganze Zahl, so ist $a \equiv A$; ist es aber eine gebrochene Zahl, so sei die nächstgrössere ganze Zahl (oder wenn der Bruch negativ ist, die nächstkleinere, ohne Rücksicht auf das Vorzeichen) gleich k; dann wird $A+km$ zwischen a und $a+m$ liegen und daher die gesuchte Zahl sein. Offenbar aber liegen die Quotienten

$$\frac{a-A}{m},\ \frac{a+1-A}{m},\ \frac{a+2-A}{m}, \ldots$$

sämtlich zwischen $k-1$ und $k+1$; daher kann nicht mehr als einer von ihnen eine ganze Zahl sein.

Kleinste Reste.

4.

Es wird demnach jede Zahl sowohl in der Reihe $0, 1, 2, \ldots, m-1$ wie in der Reihe $0, -1, -2, \ldots, -(m-1)$ einen Rest besitzen und zwar werden wir diese die **kleinsten Reste** nennen. Offenbar giebt es, falls nicht 0 der Rest ist, stets zwei solche, einen positiven und einen negativen. Sind dieselben der Grösse nach ungleich, so ist der eine kleiner als $\frac{m}{2}$, im andern Falle beide gleich $\frac{m}{2}$, abgesehen vom Vorzeichen. Hieraus geht hervor, dass eine jede Zahl einen Rest besitzt, der die Hälfte des Moduls nicht übersteigt und der **absolut kleinste Rest** genannt wird.

Die Zahl -13 besitzt z. B. nach dem Modul 5 den kleinsten positiven Rest 2, der zugleich der absolut kleinste Rest ist, dagegen den kleinsten negativen Rest -3. Die Zahl $+5$ ist nach dem Modul 7 ihr eigener kleinster positiver Rest, -2 dagegen der kleinste negative und zugleich absolut kleinste Rest derselben.

Elementare Sätze über die Congruenzen.

5.

Nachdem wir diese Bezeichnungen festgestellt haben, wollen wir diejenigen Eigenschaften congruenter Zahlen, die sich auf den ersten Blick darbieten, zusammenstellen.

Diejenigen Zahlen, welche nach einem zusammengesetzten Modul congruent sind, sind auch nach jedem Teiler desselben congruent.

Wenn mehrere Zahlen einer und derselben Zahl nach einem und demselben Modul congruent sind, so sind sie (nach demselben Modul) unter einander congruent.

Auch in den folgenden Sätzen wird vorausgesetzt, dass der Modul derselbe bleibt.

Congruente Zahlen haben dieselben, incongruente aber verschiedene kleinste Reste.

6.

Hat man beliebig viele Zahlen $A, B, C, \ldots$ und ebenso viele andere $a, b, c, \ldots$, welche jenen nach irgend welchem Modul congruent sind, also

$$A \equiv a,\ B \equiv b,\ \ldots,$$

so ist:

$$A + B + C + \cdots \equiv a + b + c + \cdots$$

Ist $A \equiv a$, $B \equiv b$, so ist: $A - B \equiv a - b$.

7.

Ist $A \equiv a$, so ist auch $kA \equiv ka$.

Ist k eine positive Zahl, so ist dieses nur ein besonderer Fall des Satzes im vorhergehenden Artikel, der entsteht, wenn man daselbst $A = B = C = \cdots$ und $a = b = c = \cdots$ setzt. Ist k negativ, so wird $-k$ positiv, daher $-kA \equiv -ka$ und hieraus $kA \equiv ka$.

Ist $A \equiv a$, $B \equiv b$, so ist auch $AB \equiv ab$.

Denn es ist $AB \equiv Ab \equiv ba$.

8.

Hat man beliebig viele Zahlen $A, B, C, \ldots$ und ebenso viele andere $a, b, c, \ldots$, welche jenen congruent sind, also $A \equiv a$, $B \equiv b, \ldots$, so sind auch die Producte aus den Zahlen jeder Reihe congruent, also $ABC \ldots \equiv abc \ldots$

Nach dem vorhergehenden Artikel ist $AB \equiv ab$ und aus demselben Grunde $ABC \equiv abc$; auf dieselbe Weise können beliebig viele andere Factoren hinzutreten.

Wenn alle Zahlen $A, B, C, \ldots$ gleich angenommen werden, ebenso die entsprechenden $a, b, c, \ldots$, so erhält man den **Satz:**

Ist $A \equiv a$ und k eine ganze positive Zahl, so ist $A^k \equiv a^k$.

9.

Es sei X eine algebraische Function der unbestimmten Grösse x von der Form:

$$Ax^a + Bx^b + Cx^c + \cdots,$$

wo $A, B, C, \ldots$ irgend welche ganze Zahlen, $a, b, c, \ldots$ aber ganze nicht negative Zahlen bezeichnen. Wenn alsdann der

Unbestimmten x Werte beigelegt werden, die nach einem beliebigen Modul congruent sind, so werden auch die daraus sich ergebenden Werte der Function X einander congruent sein.

Es seien f, g einander congruente Werte von x. Dann ergiebt sich aus dem vorhergehenden Artikel:

$$f^a \equiv g^a \text{ und } Af^a \equiv Ag^a; \text{ ebenso } Bf^b \equiv Bg^b \text{ u. s. w. Daher:}$$

$$Af^a + Bf^b + Cf^c + \cdots \equiv Ag^a + Bg^b + Cg^c + \cdots, \text{ w. z. b. w.}$$

Uebrigens sieht man leicht, wie sich dieser Satz auf Functionen von mehreren Unbestimmten ausdehnen lässt.

10.

Wenn demnach für x alle aufeinander folgenden ganzen Zahlen gesetzt und die Werte der Function X auf ihre kleinsten Reste gebracht werden, so werden diese eine Reihe bilden, in welcher nach einem Intervall von m Gliedern (wo m den Modul bezeichnet) immer dieselben Glieder wiederkehren, oder diese Reihe wird aus einer unendlichvielmal wiederholten **Periode** von m Gliedern gebildet sein. Ist z. B. $X = x^3 - 8x + 6$ und $m = 5$, so werden für $x = 0, 1, 2, 3 \ldots$ die Werte von X die folgenden kleinsten positiven Reste ergeben: 1, 4, 3, 4, 3, 1, 4, wo die fünf ersten 1, 4, 3, 4, 3 sich bis ins Unendliche hin wiederholen; und wenn die Reihe rückwärts fortgesetzt wird, d. h. wenn x negative Werte gegeben werden, so geht dieselbe Periode in umgekehrter Reihenfolge der Glieder hervor. Daraus ist offenbar, dass andere Glieder als die, welche diese Periode bilden, in der ganzen Reihe nicht statthaben können.

11.

In diesem Beispiel kann demnach X weder $\equiv 0$ noch $\equiv 2$ (mod. 5) und noch viel weniger $= 0$ oder $= 2$ werden. Daraus folgt, dass die Gleichungen $x^3 - 8x + 6 = 0$ und $x^3 - 8x + 4 = 0$ durch ganze Zahlen und infolge dessen, wie bekannt, durch rationale Zahlen nicht aufgelöst werden können. Allgemein ist ersichtlich, dass die Gleichung $X = 0$, wenn die Function X der Unbekannten x die Form

$$x^n + Ax^{n-1} + Bx^{n-2} + \cdots + N$$

hat, wo $A, B, C, \ldots$ ganze Zahlen sind und n eine ganze positive Zahl ist (auf welche Form bekanntlich alle algebraischen Gleichungen zurückgeführt werden können), keine rationale Wurzel hat, wenn man nicht der Congruenz $X \equiv 0$ nach irgend einem Modul Genüge leisten kann. Dieses Kriterium, welches sich uns hier unmittelbar darbot, soll im achten Abschnitt*) ausführlicher behandelt werden. Sicherlich wird man sich schon aus dieser Probe einen kleinen Begriff von dem Nutzen dieser Untersuchungen bilden können.

---

*) Vgl. das Vorwort des Herausgebers.

Gewisse Anwendungen.

12.

Auf die in diesem Kapitel angeführten Sätze gründet sich mehreres, was in der Arithmetik gelehrt zu werden pflegt, z. B. die Regeln zur Untersuchung der Teilbarkeit einer gegebenen Zahl durch 9, 11 oder durch andere Zahlen. Nach dem Modul 9 sind alle Zahlen, welche Potenzen von 10 sind, der Einheit congruent. Hat daher die gegebene Zahl die Form $a + 10b + 100c + \cdots$, so wird dieselbe denselben kleinsten Rest nach dem Modul 9 geben wie $a + b + c + \cdots$ Hieraus ist ersichtlich, dass, wenn die einzelnen Ziffern der dekadisch ausgedrückten Zahl ohne Rücksicht auf die Stelle, welche sie einnehmen, addirt werden, diese Summe und die gegebene Zahl dieselben kleinsten Reste darbieten und daher diese durch 9 geteilt werden kann, wenn jene durch 9 teilbar ist, und umgekehrt. Dasselbe gilt vom Teiler 3. Da ferner, nach dem Modul 11, $100 \equiv 1$ ist, so ist allgemein $10^{2k} \equiv 1$, $10^{2k+1} \equiv 10 \equiv -1$, und die Zahl von der Form $a + 10b + 100c + \cdots$ wird nach dem Modul 11 denselben kleinsten Rest geben wie $a - b + c - \cdots$, woraus sich sofort die bekannte Regel ergiebt. Aus demselben Prinzip lassen sich leicht alle ähnlichen Vorschriften ableiten.

Ebenso ist in dem Vorhergehenden der Grund für die Regeln zu suchen, welche man gewöhnlich zur Prüfung der Richtigkeit arithmetischer Rechnungen empfiehlt. Wenn nämlich aus gegebenen Zahlen andere durch Addition, Subtraction, Multiplikation oder Potenzerhebung abzuleiten sind, so werden an Stelle der gegebenen Zahlen die kleinsten Reste derselben nach einem willkürlichen Modul (gewöhnlich 9 oder 11, da sich in unserm dekadischen Systeme die Reste nach diesen, wie wir soeben gezeigt haben, so leicht finden lassen) gesetzt. Die aus diesen entstehenden Zahlen müssen denen, welche aus den gegebenen Zahlen abgeleitet worden waren, congruent sein. Ist dieses nicht der Fall, so folgt, dass sich ein Fehler in die Rechnung eingeschlichen habe.

Da jedoch dies und Ähnliches hinlänglich bekannt ist, so dürfte es überflüssig sein, länger dabei zu verweilen.

Zweiter Abschnitt.

Von den Congruenzen ersten Grades.

Vorbereitende Sätze über Primzahlen, Factoren u. s. w.

13.

Satz. Das Product aus zwei positiven Zahlen, welche kleiner als eine gegebene Primzahl sind, lässt sich nicht durch diese Primzahl teilen.

Es sei p eine Primzahl und a eine positive Zahl $< p$; dann wird behauptet, dass es keine positive Zahl $b < p$ von der Beschaffenheit giebt, dass $ab \equiv 0$ (mod. p) ist.

Beweis. Angenommen, es gäbe Zahlen $b, c, d, \ldots$, die sämtlich kleiner als p und von der Beschaffenheit sind, dass $ab \equiv 0$, $ac \equiv 0$, $ad \equiv 0, \ldots$, (mod. p) ist. Von allen diesen sei b die kleinste, so dass keine der Zahlen, die kleiner als b sind, jene Eigenschaft besitzt. Dann ist offenbar $b > 1$. Denn wäre $b = 1$, so würde $ab = a < p$ (nach Voraussetzung), also nicht durch p teilbar sein. Mithin lässt sich p, da es eine Primzahl ist, nicht durch b teilen, sondern wird zwischen zwei aufeinanderfolgende Vielfache von b, etwa zwischen mb und $(m+1)\,b$, fallen. Ist $p - mb = b'$, so wird b' eine positive Zahl und kleiner als b sein. Da nun nach unserer Annahme $ab \equiv 0$ (mod. p) ist, so hat man auch $mab \equiv 0$ (nach Artikel 7) und somit, wenn man dies von $ap \equiv 0$ subtrahiert: $a\,(p - mb) = ab' \equiv 0$, d. h. b' müsste zur Reihe der Zahlen $b, c, d, \ldots$ gerechnet werden, obwohl es kleiner als die kleinste b dieser Zahlen ist. Dies widerspricht aber unserer Annahme.

14.

Wenn weder a noch b durch die Primzahl p sich teilen lässt, so ist auch das Product ab durch p nicht teilbar.

Die kleinsten positiven Reste der Zahlen a, b nach dem Modul p seien α, β, von denen (nach Voraussetzung) keiner gleich 0 ist. Wäre nun $ab \equiv 0$ (mod. p), so würde auch, da $ab \equiv \alpha\beta$ ist, $\alpha\beta \equiv 0$ sein, was mit dem vorhergehenden Satze nicht verträglich ist.

Der Beweis dieses Satzes ist bereits von Euclid, *Elem. VII, 32,* gegeben worden. Wir haben ihn jedoch nicht weglassen wollen, einmal weil von den Neueren einige entweder nur nichtige Gründe für einen Beweis des Satzes ausgegeben oder ihn ganz und gar übergangen haben, sodann weil sich das Wesen der hier angewendeten Methode, deren wir uns später zur Aufsuchung viel versteckter liegender Wahrheiten bedienen werden, an einem einfacheren Beispiele leichter verstehen lässt.

15.

Wenn keine der Zahlen $a, b, c, d, \ldots$ durch die Primzahl p sich teilen lässt, so ist auch das Product $abcd \ldots$ durch p nicht teilbar.

Nach dem vorigen Artikel ist ab durch p nicht teilbar; daher auch nicht abc, daher auch nicht $abcd$ u. s. w.

16.

Satz. Jede zusammengesetzte Zahl lässt sich nur auf eine einzige Weise in Primfactoren zerlegen.

Beweis. Dass jede zusammengesetzte Zahl in Primfactoren zerlegt werden kann, ist aus den Anfangsgründen bekannt; dass dies aber nicht auf mehrere verschiedene Arten geschehen könne, wird mit Unrecht meistenteils stillschweigend angenommen. Denken wir uns, dass die zusammengesetzte Zahl A, welche gleich $a^\alpha b^\beta c^\gamma \ldots$ sei, wo $a, b, c, \ldots$ ungleiche Primzahlen bezeichnen, noch auf eine andere Weise in Primfactoren zerlegbar sei, so ist zunächst klar, dass in diesem zweiten System von Factoren andere Primzahlen als $a, b, c, \ldots$ nicht vorkommen können, da die aus letzteren zusammengesetzte Zahl A sich durch keine andere Primzahl teilen lässt. Andererseits darf aber auch in diesem zweiten System von Factoren keine der Primzahlen $a, b, c, \ldots$ fehlen, da sie ja sonst die Zahl A (nach vorigem Artikel) nicht teilen würde. Daher können sich diese beiden Zerlegungen in Factoren nur insoweit unterscheiden, dass in der einen irgend eine Primzahl öfter enthalten ist als in der andern. Es sei p eine solche Primzahl, welche in der einen Zerlegung m-mal, in der andern aber n-mal vorkommt, und es sei $m > n$. Hebt man dann den Factor p aus jedem der beiden Systeme n-mal weg, so wird er in dem einen noch $(m-n)$-mal übrig bleiben, in dem andern aber gar nicht mehr vorkommen, d. h. man erhält für die Zahl $\frac{A}{p^n}$ zwei Zerlegungen in Factoren, deren eine vom Factor p vollständig frei ist, während die andere ihn $(m-n)$-mal enthält. Dies steht aber im Widerspruch mit dem, was wir soeben bewiesen haben.

17.

Wenn daher die zusammengesetzte Zahl A das Product aus den Zahlen $B, C, D, \ldots$ ist, so ist klar, dass unter den Primfactoren der Zahlen $B, C, D, \ldots$ keine andern vorkommen können, als die, welche auch in

den Factoren der Zahl A auftreten, und dass jeder dieser Primfactoren in $B, C, D, \ldots$ zusammen ebenso oft vorkommen muss wie in A. Hieraus ergiebt sich ein Kriterium, nach welchem man entscheiden kann, ob eine Zahl B eine andere A teilt oder nicht. Jenes ist der Fall, wenn B weder andere Primfactoren, noch irgend einen öfter enthält als A. Ist irgend eine dieser Bedingungen nicht erfüllt, so ist B kein Teiler von A.

Hieraus kann man mit Hülfe der Combinationsrechnung leicht ableiten, dass, wenn

$$A = a^\alpha b^\beta c^\gamma \ldots$$

ist, wo $a, b, c, \ldots$ wie oben verschiedene Primzahlen bezeichnen, die Anzahl der verschiedenen Teiler von A mit Einschluss von 1 und A gleich

$$(\alpha + 1)(\beta + 1)(\gamma + 1) \ldots .$$

ist.

18.

Ist daher $A = a^\alpha b^\beta c^\gamma \ldots$, $K = k^\varkappa l^\lambda m^\mu \ldots$, und sind die Primzahlen $a, b, c, \ldots, k, l, m, \ldots$ sämtlich von einander verschieden, so haben offenbar A und K keinen gemeinschaftlichen Teiler ausser 1, oder sie sind zu einander prim.

Das mehreren gegebenen Zahlen $A, B, C, \ldots$ **gemeinschaftliche grösste Mass** bestimmt man folgendermassen: Man zerlege alle jene Zahlen in ihre Primfactoren und suche von diesen diejenigen heraus, welche allen Zahlen $A, B, C, \ldots$ gemeinschaftlich sind (giebt es keine solchen, so giebt es auch keinen allen gemeinschaftlichen Teiler). Sodann merke man sich, wie oft ein jeder dieser Primfactoren in den einzelnen Zahlen $A, B, C, \ldots$ enthalten ist, oder wie viel Dimensionen ein jeder in den einzelnen Zahlen $A, B, C, \ldots$ hat. Endlich gebe man jedem einzelnen Primfactor die kleinste von allen Dimensionen, welche er in $A, B, C, \ldots$ hat, und bilde aus den so erhaltenen Potenzen ein Product; dieses wird dann das gesuchte gemeinschaftliche Mass sein.

Wenn man aber das **kleinste gemeinschaftliche Vielfache** der Zahlen $A, B, C, \ldots$ haben will, so muss man folgendermassen verfahren. Man sammle alle Primzahlen, welche irgend eine der Zahlen $A, B, C, \ldots$ teilen, gebe jeder einzelnen die grösste von allen Dimensionen, welche sie in den Zahlen $A, B, C, \ldots$ hat, und bilde aus allen so erhaltenen Potenzen ein Product; dieses wird dann das gesuchte gemeinschaftliche Vielfache sein.

Beispiel. Es sei $A = 504 = 2^3 \cdot 3^2 \cdot 7$, $B = 2880 = 2^6 \cdot 3^2 \cdot 5$, $C = 864 = 2^5 \cdot 3^3$. Um den grössten gemeinschaftlichen Teiler zu finden, hat man die Primfactoren 2, 3, denen die Dimensionen 3, 2 zu geben sind, so dass derselbe gleich $2^3 \cdot 3^2 = 72$ wird. Das kleinste gemeinschaftliche Vielfache dagegen ist: $2^6 \cdot 3^3 \cdot 5 \cdot 7 = 60480$.

Die Beweise lassen wir ihrer Leichtigkeit wegen fort. Wie übrigens diese Aufgaben zu lösen sind, wenn die Zerlegung der Zahlen $A, B, C, \ldots$ in Factoren nicht gegeben ist, ist aus den Elementen bekannt.

19.

Wenn die Zahlen $a, b, c, \ldots$ zu einer andern k prim sind, so ist auch das Product aus jenen $abc\ldots$ prim zu k.

Denn da keine der Zahlen $a, b, c, \ldots$ mit k einen Primfactor gemeinschaftlich hat und das Product $abc\ldots$ nur die Primfactoren haben kann, welche Factoren irgend einer der Zahlen $a, b, c, \ldots$ sind, so hat auch das Product $abc\ldots$ mit k keinen Primfactor gemeinschaftlich. Daher sind k und $abc\ldots$ nach dem vorhergehenden Artikel prim zu einander.

Wenn die Zahlen $a, b, c, \ldots$ prim zu einander sind und einzeln eine andere Zahl k teilen, so ist auch das Product aus jenen ein Teiler der Zahl k.

Dies ergiebt sich ebenso leicht aus den Artikeln 17 und 18. Denn ist p ein beliebiger Primteiler des Productes $abc\ldots$, und ist derselbe π-mal darin enthalten, so muss offenbar irgend eine der Zahlen $a, b, c, \ldots$ denselben Teiler ebenfalls π-mal enthalten. Daher enthält auch k, welches durch jene Zahl geteilt wird, π-mal den Teiler p. Analoges gilt von den übrigen Teilern des Productes $abc\ldots$

Wenn daher zwei Zahlen m, n nach mehreren zu einander primen Moduln $a, b, c, \ldots$ congruent sind, so werden sie auch nach dem Producte aus diesen einander congruent sein.

Denn da $m-n$ durch jede einzelne der Zahlen $a, b, c, \ldots$ teilbar ist, so ist es auch durch das Product derselben teilbar.

Wenn endlich a zu b prim und ak durch b teilbar ist, so wird auch k durch b teilbar sein.

Denn da ak sowohl durch a als auch durch b teilbar ist, so ist es auch durch das Product ab teilbar, d. h. es ist $\frac{ak}{ab} = \frac{k}{b}$ eine ganze Zahl.

20.

Sobald die Zahl $A = a^\alpha b^\beta c^\gamma \ldots$, wo $a, b, c, \ldots$ einander ungleiche Primzahlen bezeichnen, irgend eine Potenz ist, etwa $A = k^n$, so werden sämtliche Exponenten $\alpha, \beta, \gamma, \ldots$ durch n teilbar sein.

Denn die Zahl k enthält keine andern Primfactoren als $a, b, c, \ldots$, und zwar enthält sie alle diese. Kommt der Factor a darin α'-mal vor, so wird dieser Faktor in k^n oder A $n\alpha'$-mal vorkommen. Daher ist $n\alpha' = \alpha$ und $\frac{\alpha}{n}$ eine ganze Zahl. Ebenso beweist man, dass $\frac{\beta}{n}, \ldots$ ganze Zahlen sind.

21.

Wenn $a, b, c, \ldots$ prim zu einander sind, und das Product $abc\ldots$ irgend eine Potenz, etwa $abc\ldots = k^n$, ist, so werden die einzelnen Zahlen $a, b, c, \ldots$ gleichfalls Potenzen sein.

Es sei $a = l^\lambda m^\mu p^\pi \ldots$, wo $l, m, p, \ldots$ von einander verschiedene Prim-

zahlen bezeichnen, von denen nach Voraussetzung keine ein Factor der Zahlen b, c, ... ist. Daher wird das Product abc ... den Factor l λ-mal, den Factor m μ-mal u. s. w. enthalten. Somit sind (nach vorigem Artikel) λ, μ, π, ... durch n teilbar, und daher ist

$$\sqrt[n]{a} = l^{\frac{\lambda}{n}} m^{\frac{\mu}{n}} p^{\frac{\pi}{n}} \ldots$$

eine ganze Zahl. Dasselbe gilt bezüglich der Zahlen b, c, ...

Diese Sätze über die Primzahlen mussten wir zuerst vorausschicken. Jetzt wenden wir uns zu denen, die zu unserem Ziele in näherer Beziehung stehen.

22.

Wenn die Zahlen a, b durch eine andere k teilbar und nach dem zu k primen Modul m einander congruent sind, so sind auch $\frac{a}{k}$ und $\frac{b}{k}$ nach demselben Modul einander congruent.

Denn offenbar ist $a - b$ durch k und, nach Voraussetzung, auch durch m teilbar; daher ist (nach Artikel 19) $\frac{a-b}{k}$ durch m teilbar, d. h. es ist $\frac{a}{k} \equiv \frac{b}{k}$ (mod. m).

Wenn aber, unter sonst gleichen Voraussetzungen, m und k den grössten gemeinschaftlichen Teiler e haben, so ist $\frac{a}{k} \equiv \frac{b}{k}$ $\left(\text{mod. } \frac{m}{e}\right)$.

Denn $\frac{k}{e}$ und $\frac{m}{e}$ sind prim zu einander. Da aber $a - b$ sowohl durch k als durch m und daher auch $\frac{a-b}{e}$ sowohl durch $\frac{k}{e}$ als durch $\frac{m}{e}$ und somit durch $\frac{km}{e^2}$ teilbar ist, so ist auch $\frac{a-b}{k}$ durch $\frac{m}{e}$ teilbar, oder $\frac{a}{k} \equiv \frac{b}{k}$ $\left(\text{mod. } \frac{m}{e}\right)$.

23.

Wenn a prim zu m ist, und e, f nach dem Modul m incongruente Zahlen sind, so werden auch ae und af nach dem Modul m incongruent sein.

Dieser Satz ist nur eine Umkehrung des Satzes im vorhergehenden Artikel.

Hieraus aber geht hervor, dass, wenn a mit sämtlichen ganzen Zahlen von 0 bis $m - 1$ multipliciert wird und die Producte nach dem Modul m auf ihre kleinsten Reste gebracht werden, diese letzteren sämtlich von einander verschieden sind. Und da die Anzahl dieser Reste, von denen keiner grösser als m ist, gleich m ist, und es ebenso viele Zahlen von 0

bis $m-1$ giebt, so folgt, dass keine dieser Zahlen unter jenen Resten fehlen kann.

24.

Der Ausdruck $ax+b$, in welchem a, b gegebene Zahlen und x eine unbestimmte oder veränderliche Zahl bezeichnet, kann nach dem zu a primen Modul m jeder beliebigen gegebenen Zahl congruent werden.

Die Zahl, welcher jener Ausdruck congruent werden soll, sei c und der kleinste positive Rest von $c-b$ nach dem Modul m sei e. Dann giebt es nach dem vorhergehenden Artikel notwendig einen Wert von $x<m$ von solcher Beschaffenheit, dass der kleinste Rest des Products ax nach dem Modul m gleich e ist. Ist v dieser Wert, so hat man $av \equiv e \equiv c-b$, mithin $av+b \equiv c$ (mod. m).

25.

Den Ausdruck, welcher zwei congruente Grössen nach Analogie einer Gleichung mit einander verbindet, nennen wir eine **Congruenz**. Enthält dieselbe eine Unbekannte, so heisst die Congruenz gelöst, wenn man für diese Unbekannte einen der Congruenz genügenden Wert (**Wurzel**) findet. Hieraus erkennt man ferner, was eine auflösbare und eine nicht auflösbare Congruenz ist. Endlich sieht man leicht, dass hier ähnliche Unterscheidungen stattfinden können, wie bei den Gleichungen. Von transcendenten Congruenzen werden weiter unten Beispiele vorkommen; die algebraischen aber werden je nach der höchsten in ihnen enthaltenen Potenz der Unbekannten in Congruenzen ersten, zweiten und höheren Grades eingeteilt. Ebenso können auch mehrere Congruenzen mit mehreren Unbekannten, über deren Elimination das Nähere mitzuteilen sein wird, gegeben sein.

Auflösung der Congruenzen ersten Grades.

26.

Die Congruenz ersten Grades $ax+b \equiv c$ ist nach Artikel 24 stets auflösbar, wenn der Modul zu a prim ist. Ist v ein passender Wert von x oder eine Wurzel der Congruenz, so werden offenbar alle Zahlen, welche v nach dem Modul der gegebenen Congruenz congruent sind, auch Wurzeln sein (Artikel 9). Ebenso leicht sieht man, dass alle Wurzeln v congruent sein müssen; denn ist t eine andere Wurzel, so ist $av+b \equiv at+b$, daher $av \equiv at$ und somit $v \equiv t$ (Artikel 22). Hieraus folgt, dass die Congruenz $x \equiv v$ (mod. m) die vollständige Lösung der Congruenz $ax+b \equiv c$ darstellt.

Da die Lösungen der Congruenz durch Werte, welche x congruent sind, auf der Hand liegen und in dieser Hinsicht congruente Zahlen als äquivalent zu betrachten sind, so werden wir derartige Lösungen der Congruenz für eine und dieselbe halten. Wenn daher unsere Congruenz $ax+b \equiv c$ andere Lösungen nicht zulässt, so werden wir sagen, dass sie

nur auf eine einzige Weise lösbar sei oder nur eine einzige Wurzel habe. So besitzt z. B. die Congruenz $6x + 5 \equiv 13 \pmod{11}$ keine andern Wurzeln als die, welche $\equiv 5 \pmod{11}$ sind. Anders verhält sich die Sache bei Congruenzen höherer Grade oder bei Congruenzen ersten Grades, in denen die Unbekannte mit einer Zahl multipliciert ist, zu welcher der Modul nicht prim ist.

27.

Es bleibt uns noch übrig, über die Auffindung der Lösung einer derartigen Congruenz einiges hinzuzufügen.

Zunächst bemerken wir, dass die Congruenz $ax + t \equiv u$, deren Modul wir zu a prim voraussetzen, von der Congruenz $ax \equiv \pm 1$ abhängt. Denn wenn diese durch $x \equiv r$ befriedigt wird, so wird jener durch $x \equiv \pm (u - t)r$ genügt. Der Congruenz $ax \equiv \pm 1$ ist aber, wenn man den Modul mit b bezeichnet, die unbestimmte Gleichung $ax = by \pm 1$ äquivalent, und wie diese zu lösen sei, ist heutzutage hinreichend bekannt. Wir begnügen uns daher, hier den Algorithmus der Rechnung herzusetzen.

Wenn die Grössen $A, B, C, D, E, \ldots$ so von den Grössen $\alpha, \beta, \gamma, \delta, \ldots$ abhängen, dass man hat:

$$A = \alpha,\ B = \beta A + 1,\ C = \gamma B + A,\ D = \delta C + B,\ E = \varepsilon D + C,\ \ldots,$$

so bezeichnen wir sie der Kürze wegen in folgender Weise:

$$A = [\alpha],\ B = [\alpha, \beta],\ C = [\alpha, \beta, \gamma],\ D = [\alpha, \beta, \gamma, \delta],\ \ldots ^{*)}$$

Es sei nun die unbestimmte Gleichung $ax = by \pm 1$, in welcher a, b positiv sind, vorgelegt. Wir nehmen, was erlaubt ist, an, dass a nicht kleiner als b sei. Dann bilden wir nach Art des bekannten Algorithmus, durch welchen man den grössten gemeinschaftlichen Teiler zweier Zahlen sucht, mittelst gewöhnlicher Division die Gleichungen:

$$a = \alpha b + c,\ b = \beta c + d,\ c = \gamma d + e,\ \ldots,$$

so dass $\alpha, \beta, \gamma, \ldots, c, d, e, \ldots$ positive ganze Zahlen sind und $b, c, d, e, \ldots$ fortwährend abnehmen, bis wir zu einer Gleichung von der Form

$$m = \mu n + 1$$

gelangen, was bekanntlich einmal eintreten muss. Dann ist:

---

*) Diese Beziehung lässt sich noch viel allgemeiner betrachten, was wir vielleicht bei einer andern Gelegenheit thun werden. Hier fügen wir nur zwei Sätze bei, die bei der gegenwärtigen Untersuchung Anwendung finden, nämlich:

(1) $[\alpha, \beta, \gamma, \ldots, \lambda, \mu] \cdot [\beta, \gamma, \ldots, \lambda] - [\alpha, \beta, \gamma, \ldots, \lambda] \cdot [\beta, \gamma, \ldots, \lambda, \mu] = \pm 1$,

wo das obere oder untere Zeichen zu nehmen ist, je nachdem die Anzahl der Zahlen $\alpha, \beta, \gamma, \ldots, \lambda, \mu$ gerade oder ungerade ist.

(2) Die Reihenfolge der Zahlen $\alpha, \beta, \gamma, \ldots$ kann umgekehrt werden, also:

$$[\alpha, \beta, \gamma, \ldots, \lambda, \mu] = [\mu, \lambda, \ldots, \gamma, \beta, \alpha].$$

Die Beweise, welche nicht schwer sind, unterdrücken wir hier.

$$a = [n, \mu, \ldots, \gamma, \beta, \alpha], \quad b = [n, \mu, \ldots, \gamma, \beta].$$

Nimmt man sodann

$$x = [\mu, \ldots, \gamma, \beta] \qquad y = [\mu, \ldots, \gamma, \beta, \alpha],$$

so wird $ax = by + 1$, wenn die Anzahl der Zahlen $\alpha, \beta, \gamma, \ldots, \mu, n$ gerade, dagegen $ax = by - 1$, wenn sie ungerade ist.

28.

Die allgemeine Auflösung derartiger unbestimmter Gleichungen hat zuerst Euler gelehrt, *Comment. Petrop. T. VII p. 46.**) Die Methode, deren er sich bediente, besteht in der Substitution anderer Unbekannten an Stelle von x, y und ist heutzutage hinreichend bekannt. Lagrange griff die Sache ein wenig anders an: Aus der Theorie der Kettenbrüche nämlich ist bekannt, dass, wenn man den Bruch $\frac{a}{b}$ in einen Kettenbruch

$$\cfrac{1}{\alpha + \cfrac{1}{\beta + \cfrac{1}{\gamma + \cdots + \cfrac{1}{\mu + \cfrac{1}{n}}}}}$$

verwandelt und diesen nach Weglassung seines letzten Gliedes $\frac{1}{n}$ wieder zu einem gewöhnlichen Bruche $\frac{x}{y}$ macht, $ax = by \pm 1$ ist, falls a prim zu b ist. Uebrigens ergiebt sich aus beiden Methoden derselbe Algorithmus. Die Untersuchungen von Lagrange finden sich in *Hist. de l'Ac. de Berlin Année 1767 p. 175* und nebst andern in den Zusätzen zur französischen Übersetzung von Euler's Algebra.

29.

Die Congruenz $ax + t \equiv u$, deren Modul nicht prim zu a ist, lässt sich leicht auf den vorhergehenden Fall zurückführen. Es sei m der Modul und δ der grösste gemeinschaftliche Teiler der Zahlen a, m. Zunächst ist klar, dass jeder der Congruenz nach dem Modul m genügende Wert von x derselben auch nach dem Modul δ genügt (Artikel 5). Es ist aber immer $ax \equiv 0 \pmod{\delta}$, da δ ein Teiler von a ist. Daher ist die vorgelegte Congruenz nur lösbar, wenn $t \equiv u \pmod{\delta}$, d. h. $t - u$ durch δ teilbar ist.

Setzen wir daher $a = \delta e$, $m = \delta f$, $t - u = \delta k$, so wird e zu f prim sein, und der gegebenen Congruenz $\delta ex + \delta k \equiv 0 \pmod{\delta f}$ wird die folgende $ex + k \equiv 0 \pmod{f}$ äquivalent sein, d. h. jeder Wert von x, welcher dieser genügt, wird auch jener genügen und umgekehrt. Denn offenbar lässt

*) Vgl. die Zusätze am Schlusse der Disquisitiones.

sich $ex+k$ durch f teilen, wenn sich $\delta ex+\delta k$ durch δf teilen lässt und umgekehrt. Die Congruenz $ex+k\equiv 0$ (mod. f) haben wir aber oben auflösen gelehrt, woraus zugleich folgt, dass, wenn v einer der Werte von x ist, $x\equiv v$ (mod. f) die vollständige Lösung der gegebenen Congruenz darstellt.

30.

Wenn der Modul zusammengesetzt ist, ist es zuweilen besser, sich folgender Methode zu bedienen.

Es sei der Modul $=mn$ und die gegebene Congruenz $ax\equiv b$. Man löse zunächst diese Congruenz nach dem Modul m und nehme an, dass ihr genügt werde, wenn $x\equiv v\left(\text{mod.}\,\frac{m}{\delta}\right)$ ist, wo δ den grössten gemeinschaftlichen Teiler der Zahlen m und a bezeichnet. Nun ist klar, dass jeder der Congruenz $ax\equiv b$ nach dem Modul mn genügende Wert von x derselben auch nach dem Modul m genügen muss und daher in der Form $v+\frac{m}{\delta}x'$ enthalten ist, wo x' eine unbestimmte Zahl bezeichnet, obwohl nicht umgekehrt alle in der Form $v+\frac{m}{\delta}x'$ enthaltenen Zahlen der Congruenz nach dem Modul mn genügen. Wie aber x' bestimmt werden muss, damit $v+\frac{m}{\delta}x'$ eine Wurzel der Congruenz $ax\equiv b$ (mod. mn) werde, lässt sich aus der Lösung der Congruenz $\frac{am}{\delta}x'+av\equiv b$ (mod. mn), welcher die folgende $\frac{a}{\delta}x'\equiv\frac{b-av}{m}$ (mod. n) äquivalent ist, ersehen. Es folgt hieraus, dass die Lösung jeder beliebigen Congruenz ersten Grades nach dem Modul mn zurückgeführt werden kann auf die Lösung zweier Congruenzen nach den Moduln m und n. Man erkennt leicht, dass, wenn n wiederum das Product aus zwei Factoren ist, die Lösung der Congruenz nach dem Modul n von der Lösung zweier Congruenzen abhängt, deren Moduln jene Factoren sind. Allgemein hängt die Lösung einer Congruenz nach irgend einem zusammengesetzten Modul von der Lösung anderer Congruenzen ab, deren Moduln Factoren jener Zahl sind. Diese letzteren können aber, wenn es zweckmässig erscheint, immer so angenommen werden, dass sie Primzahlen sind.

Beispiel. Ist die Congruenz $19x\equiv 1$ (mod. 140) vorgelegt, so löse man sie zunächst nach dem Modul 2, wodurch sich ergiebt $x\equiv 1$ (mod. 2). Setzt man $x=1+2x'$, so wird $38x'\equiv -18$ (mod. 140), welcher die folgende: $19x'\equiv -9$ (mod. 70) äquivalent ist. Löst man diese letztere wiederum nach dem Modul 2, so wird $x'\equiv 1$ (mod. 2) und daher, wenn $x'=1+2x''$ gesetzt wird: $38x''\equiv -28$ (mod. 70) oder $19x''\equiv -14$ (mod. 35). Diese nach dem Modul 5 gelöst giebt: $x''\equiv 4$ (mod. 5), und wenn man $x''=4+5x'''$ setzt, so wird: $95x'''\equiv -90$ (mod. 35) oder: $19x'''\equiv -18$ (mod. 7). Aus dieser endlich folgt: $x'''\equiv 2$ (mod. 7), und wenn man

$x'' = 2 + 7x'''$ setzt, so findet man $x = 59 + 140x'''$. Daher ist $x \equiv 59$ (mod. 140) die vollständige Lösung der vorgelegten Congruenz.

31.

In ähnlicher Weise, wie die Wurzel der Gleichung $ax = b$ durch $\frac{b}{a}$ ausgedrückt wird, werden wir auch irgend eine Wurzel der Congruenz $ax \equiv b$ mit $\frac{b}{a}$ bezeichnen und den Modul der Congruenz der Deutlichkeit halber hinzusetzen. So bezeichnet z. B. $\frac{19}{17}$ (mod. 12) jede Zahl, welche $\equiv 11$ (mod. 12) ist (was auch der Analogie nach durch $\frac{11}{1}$ (mod. 12) bezeichnet werden kann). Allgemein geht aus dem Vorhergehenden hervor, dass $\frac{b}{a}$ (mod. c) keine reelle Bedeutung hat (oder, wenn man lieber will, ein imaginärer Ausdruck ist), wenn a und c einen gemeinschaftlichen Teiler haben, der nicht zugleich auch b teilt. Abgesehen von diesem Falle aber wird der Ausdruck $\frac{b}{a}$ (mod. c) stets reelle Werte haben und zwar unendlich viele; letztere aber werden sämtlich nach dem Modul c congruent sein, wenn a prim zu c ist, oder nach dem Modul $\frac{c}{\delta}$, wenn δ der grösste gemeinschaftliche Teiler der Zahlen c und a ist.

Mit diesen Ausdrücken kann man fast ebenso rechnen, wie mit den gewöhnlichen Brüchen. Einige Eigenschaften, die sich leicht aus dem Vorhergehenden ableiten lassen, setzen wir hierher.

1. Wenn nach dem Modul c $a \equiv \alpha$, $b \equiv \beta$ ist, so sind die Ausdrücke $\frac{a}{b}$ (mod. c) und $\frac{\alpha}{\beta}$ (mod. c) äquivalent.

2. $\frac{a\delta}{b\delta}$ (mod. $c\delta$) und $\frac{a}{b}$ (mod. c) sind äquivalent.

3. $\frac{ak}{bk}$ (mod. c) und $\frac{a}{b}$ (mod. c) sind äquivalent, wenn k prim zu c ist.

Wir könnten noch viele andere ähnliche Sätze anführen; da dieselben aber keine Schwierigkeit bieten und für das Folgende nicht so nötig sind, gehen wir zu etwas anderem über.

Die Zahl zu finden, welche gegebenen Resten nach gegebenen Moduln congruent ist.

32.

Die Aufgabe, welche im Folgenden oft zur Anwendung kommen wird, nämlich: Alle Zahlen zu finden, welche nach beliebig vielen gegebenen Moduln gegebene Reste lassen, kann mit Hülfe des Vorhergehenden leicht gelöst werden. Es seien zunächst zwei Moduln A und B ge-

geben, nach denen eine gesuchte Zahl z den Zahlen a und b respective congruent sein soll. Es sind daher alle Werte von z unter der Form $Ax+a$ enthalten, wo x eine unbestimmte Zahl, aber von solcher Beschaffenheit ist, dass $Ax+a\equiv b$ (mod. B) wird. Wenn nun δ der grösste gemeinschaftliche Teiler der Zahlen A und B ist, so wird die vollständige Lösung dieser Congruenz die folgende Form haben $x\equiv v\left(\text{mod.}\,\frac{B}{\delta}\right)$, oder es wird, was auf dasselbe hinauskommt, $x=v+\frac{kB}{\delta}$ sein, wo k eine willkürliche ganze Zahl bezeichnet. Somit wird die Formel $Av+a+\frac{kAB}{\delta}$ alle Werte von z umfassen, d. h. $z\equiv Av+a\left(\text{mod.}\,\frac{AB}{\delta}\right)$ wird die vollständige Lösung des Problems sein. — Kommt zu den Moduln A, B noch ein dritter C hinzu, nach welchem die gesuchte Zahl z congruent c sein soll, so muss man offenbar in derselben Weise weiter verfahren, da die beiden früheren Bedingungen bereits in eine einzige zusammengefasst sind. Ist also ε der grösste gemeinschaftliche Teiler der Zahlen $\frac{AB}{\delta}$ und C und $x\equiv w\left(\text{mod.}\,\frac{C}{\varepsilon}\right)$ die Lösung der Congruenz $\frac{AB}{\delta}x+Av+a\equiv c$ (mod. C), so wird die Aufgabe durch die Congruenz $z\equiv\frac{ABw}{\delta}+Av+a\left(\text{mod.}\,\frac{ABC}{\delta\varepsilon}\right)$ vollständig gelöst sein. — In ähnlicher Weise hat man zu verfahren, wie viele Moduln auch immer gegeben sein mögen. Es mag bemerkt werden, dass $\frac{AB}{\delta}$, $\frac{ABC}{\delta\varepsilon}$ die kleinsten gemeinschaftlichen Vielfachen resp. der Zahlen A, B und A, B, C sind; man erkennt hieraus leicht, dass, wie viele Moduln A, B, C, ... auch vorhanden sein mögen, die vollständige Lösung die folgende Form haben wird: $z\equiv r$ (mod. M), wo M der kleinste gemeinschaftliche Dividuus jener Zahlen ist. Ist ferner irgend eine der Hülfscongruenzen unlösbar, so folgt daraus, dass das Problem eine Unmöglichkeit in sich schliesst. Offenbar aber kann dies nicht der Fall sein, wenn alle Zahlen A, B, C, ... unter einander prim sind.

Beispiel. Die Zahlen A, B, C; a, b, c seien resp. 504, 35, 16; 17, -4, 33. Hier sind die beiden Bedingungen, dass $z\equiv 17$ (mod. 504) und $\equiv -4$ (mod. 35) sein solle, der einen: $z\equiv 521$ (mod. 2520) äquivalent. Letztere, mit der folgenden: $z\equiv 33$ (mod. 16) verbunden, liefert $z\equiv 3041$ (mod. 5040).

33.

Sind alle Zahlen A, B, C, ... zu einander prim, so ist bekanntlich das Product aller das kleinste gemeinschaftliche Vielfache derselben. In diesem Falle werden offenbar alle Congruenzen $z\equiv a$ (mod. A), $z\equiv b$ (mod. B), ... einer einzigen $z\equiv r$ (mod. R), in welcher R das Product der

Zahlen A, B, C, ... bezeichnet, vollkommen äquivalent sein. Hieraus folgt umgekehrt, dass die eine Bedingung $z \equiv r$ (mod. R) in mehrere zerlegt werden kann. Wenn nämlich R auf irgend eine Weise in zu einander prime Factoren A, B, C, ... zerlegt ist, so werden die Bedingungen $z \equiv r$ (mod. A), $z \equiv r$ (mod. B), $z \equiv r$ (mod. C), ... die gegebene vollständig erschöpfen. Diese Bemerkung eröffnet uns einen Weg, nicht nur die Unmöglichkeit der Aufgabe, falls sich eine solche etwa aus den gegebenen Bedingungen ergeben sollte, sofort zu erkennen, sondern auch die Rechnung bequemer und kürzer durchzuführen.

34.

Die gegebenen Bedingungen seien wie oben: $z \equiv a$ (mod. A), $z \equiv b$ (mod. B), $z \equiv c$ (mod. C), ... Man löse sämtliche Moduln in zu einander prime Factoren, A in $A'A''A'''$ ..., B in $B'B''B'''$ ... u. s. w. und zwar derart auf, dass die Zahlen A', A'', ..., B', B'', ... entweder Primzahlen oder Potenzen von Primzahlen sind. Ist daher eine der Zahlen A, B, C, ... schon an sich eine Primzahl oder die Potenz einer solchen, so ist für diese eine Zerlegung in Factoren nicht nötig. Dann ergiebt sich aus dem Vorhergehenden, dass man für die gegebenen Bedingungen die folgenden substituieren kann:

$$z \equiv a \text{ (mod. } A'), \quad z \equiv a \text{ (mod. } A''), \quad z \equiv a \text{ (mod. } A'''), \ldots$$
$$z \equiv b \text{ (mod. } B'), \quad z \equiv b \text{ (mod. } B''), \quad z \equiv b \text{ (mod. } B'''), \ldots$$

u. s. w.

Wären nun nicht sämtliche Zahlen A, B, C, ... zu einander prim, z. B. A nicht prim zu B, so könnten offenbar nicht alle Primteiler von A und B von einander verschieden sein, vielmehr müsste unter den Factoren A', A'', A''', ... der eine oder der andere vorkommen, welcher unter den Factoren B', B'', B''', ... einen sich gleichen oder ein Vielfaches oder einen genauen Teil von sich hätte. Wäre zuerst $A' = B'$, so müssten die Bedingungen $z \equiv a$ (mod. A') und $z \equiv b$ (mod. B') identisch oder also $a \equiv b$ (mod. A' oder B') sein, so dass eine von diesen beiden weggelassen werden könnte. Wäre aber a nicht $\equiv b$ (mod. A'), so würde die Aufgabe etwas Unmögliches verlangen. Wenn zweitens B' ein Vielfaches von A' wäre, so müsste die Bedingung $z \equiv a$ (mod. A') in der folgenden $z \equiv b$ (mod. B') enthalten, oder es müsste die aus der letzteren folgende $z \equiv b$ (mod. A') mit der ersteren identisch sein. Hieraus folgt, dass die Bedingung $z \equiv a$ (mod. A'), falls sie nicht mit den andern im Widerspruch steht (in welchem Falle das Problem unmöglich ist), weggelassen werden kann. Sind auf diese Weise alle überflüssigen Bedingungen weggelassen, so werden offenbar alle Moduln, welche von A', A'', A''', ..., B', B'', B''', ... u. s. w. noch übrig bleiben, prim zu einander sein. Wir können alsdann hinsichtlich der Möglichkeit des Problems sicher sein und nach den vorher angegebenen Vorschriften verfahren.

35.

Beispiel. Soll wie oben $z \equiv 17 \pmod{504}$, $\equiv -4 \pmod{35}$ und $\equiv 33 \pmod{16}$ sein, so lassen sich diese Bedingungen in die folgenden zerlegen:

$$z \equiv 17 \pmod{8}, \quad \equiv 17 \pmod{9}, \quad \equiv 17 \pmod{7}$$
$$z \equiv -4 \pmod{5}, \quad \equiv -4 \pmod{7}$$
$$z \equiv 33 \pmod{16}.$$

Von diesen können die Bedingungen: $z \equiv 17 \pmod{8}$ und $z \equiv 17 \pmod{7}$ weggelassen werden, da die erstere in der Bedingung $z \equiv 33 \pmod{16}$ enthalten, die letztere aber mit $z \equiv -4 \pmod{7}$ identisch ist. Es bleiben daher die folgenden Bedingungen:

$$z \equiv \begin{cases} 17 \pmod{9} \\ -4 \pmod{5} \\ -4 \pmod{7} \\ 33 \pmod{16}, \end{cases}$$

aus denen $z \equiv 3041 \pmod{5040}$ folgt.

Überdies ist klar, dass es meistens bequemer sein wird, wenn man von den übrig bleibenden Bedingungen diejenigen, welche aus einer und derselben Bedingung hervorgegangen waren, wieder für sich zusammennimmt. Sind z. B. von den Bedingungen $z \equiv a \pmod{A'}$, $z \equiv a \pmod{A''}$, ... einige weggelassen worden, so wird die aus den übrigen zusammengesetzte die folgende sein: $z \equiv a$ nach einem Modul, welcher das Product aller von A', A'', A''', ... noch übrig gebliebenen Moduln ist. So wird in unserm Beispiel aus den Bedingungen $z \equiv -4 \pmod{5}$, $z \equiv -4 \pmod{7}$ gerade die, aus welcher sie entstanden waren, nämlich $z \equiv -4 \pmod{35}$, ohne Weiteres wieder hergestellt. Ferner folgt hieraus, dass es mit Rücksicht auf die Kürze der Rechnung nicht völlig gleichgültig ist, welche von den überflüssigen Bedingungen weggelassen wird; doch liegt es nicht in unserer Absicht, auf diese und andere practische Kunstgriffe, welche leichter durch Übung als durch besondere Vorschriften zu lernen sind, an dieser Stelle näher einzugehen.

36.

Wenn sämtliche Moduln $A, B, C, D, \ldots$ unter sich prim sind, so ist es oft besser, sich der folgenden Methode zu bedienen. Man bestimme eine Zahl α, welche nach A der Einheit, nach dem Producte der übrigen Moduln aber der Null congruent ist, oder es sei α ein beliebiger (meistens ist es vorteilhaft den kleinsten zu nehmen) mit $BCD\ldots$ multiplicierter Wert des Ausdrucks $\frac{1}{BCD\ldots} \pmod{A}$ (Siehe Artikel 32). Ebenso sei $\beta \equiv 1 \pmod{B}$ und $\equiv 0 \pmod{ACD\ldots}$, $\gamma \equiv 1 \pmod{C}$ und $\equiv 0 \pmod{ABD\ldots}$ u. s. w. Wenn dann eine Zahl z gesucht wird, welche nach den Moduln $A, B, C, D, \ldots$ respective den Zahlen $a, b, c, d, \ldots$ congruent ist, so kann man setzen:

$$z \equiv \alpha a + \beta b + \gamma c + \delta d + \cdots \pmod{ABCD\ldots}$$

Augenscheinlich nämlich ist $\alpha a \equiv a$ (mod. A), während die übrigen Glieder βb, γc, ... sämtlich $\equiv 0$ (mod. A) sind; daher ist $z \equiv a$ (mod. A). Analog ist der Beweis bezüglich der übrigen Moduln. Diese Lösung ist der früheren vorzuziehen, wenn mehrere derartige Probleme zu lösen sind, für welche die Moduln A, B, C, ... ihre Werte beibehalten; denn dann erhalten die Zahlen α, β, γ, ... constante Werte. Dies ist der Fall bei einem Problem der Zeitrechnung, bei welchem gefragt wird, das wievielste Jahr in der Julianischen Periode eine gegebene Römer-Zinszahl, güldene Zahl und Sonnenzirkel besitze. Hierbei ist $A = 15$, $B = 19$, $C = 28$. Da nun der Wert des Ausdrucks $\frac{1}{19 \cdot 28}$ (mod. 15) oder $\frac{1}{532}$ (mod. 15) gleich 13 ist, so ist $\alpha = 6916$. Analog findet man $\beta = 4200$ und $\gamma = 4845$. Demnach ist die gesuchte Zahl der kleinste Rest der Zahl $6916a + 4200b + 4845c$, wo a die Römer-Zinszahl, b die güldene Zahl und c den Sonnenzirkel bezeichnet.

Lineare Congruenzen mit mehreren Unbekannten.

37.

Das Vorhergehende möge hinsichtlich der Congruenzen ersten Grades mit einer einzigen Unbekannten genügen. Wir haben aber noch über Congruenzen zu handeln, in denen mehrere Unbekannte vorkommen. Da aber dieser Abschnitt, falls wir die Einzelheiten mit aller Strenge auseinandersetzen wollten, nicht ohne Weitschweifigkeit durchgeführt werden kann, und es hier nicht in unserer Absicht liegt, eine erschöpfende Darstellung zu geben, wir vielmehr nur das anführen wollen, was der Aufmerksamkeit am würdigsten zu sein scheint, so werden wir unsere Untersuchung hier auf wenige Bemerkungen beschränken und uns eine eingehendere Darlegung dieses Gegenstandes für eine andere Gelegenheit vorbehalten.

1. In analoger Weise wie bei Gleichungen erkennt man, dass man auch hier ebensoviele Gleichungen haben muss, als Unbekannte zu bestimmen sind.

2. Es seien also ebensoviele Congruenzen

$$\begin{array}{ll} (A) & ax + by + cz + \cdots \equiv f \pmod{m} \\ (A') & a'x + b'y + c'z + \cdots \equiv f' \\ (A'') & a''x + b''y + c''z + \cdots \equiv f'' \\ & \cdots\cdots\cdots\cdots \end{array}$$

gegeben, als Unbekannte x, y, z, ... vorhanden sind.

Man bestimme nun Zahlen ξ, ξ', ξ'', ... vermittelst der Gleichungen

$$\begin{array}{l} b\xi + b'\xi' + b''\xi'' + \cdots = 0 \\ c\xi + c'\xi' + c''\xi'' + \cdots = 0 \\ \cdots\cdots\cdots\cdots \end{array}$$

und zwar so, dass sie sämtlich ganze Zahlen werden und keinen gemeinschaftlichen Factor haben, was, wie aus der Theorie der linearen Gleichungen

bekannt ist, immer möglich ist. In ähnlicher Weise bestimme man Zahlen $v, v', v'', \ldots, \zeta, \zeta', \zeta'', \ldots$ mittelst der Gleichungen:

$$\begin{array}{l} av + a'v' + a''v'' + \cdots = 0 \\ cv + c'v' + c''v'' + \cdots = 0 \\ \cdots\cdots\cdots \\ a\zeta + a'\zeta' + a''\zeta'' + \cdots = 0 \\ b\zeta + b'\zeta' + b''\zeta'' + \cdots = 0 \\ \cdots\cdots\cdots \end{array}$$

3. Werden die Congruenzen $A, A', A'', \ldots$ zuerst resp. mit $\xi, \xi', \xi'', \ldots$, sodann mit $v, v', v'', \ldots$ u. s. w. multipliciert und sodann die Producte jedesmal addiert, so werden sich offenbar folgende Congruenzen ergeben:

$$\begin{array}{l} (a\xi + a'\xi' + a''\xi'' + \cdots)\, x \equiv f\xi + f'\xi' + f''\xi'' + \cdots \\ (bv + b'v' + b''v'' + \cdots)\, y \equiv fv + f'v' + f''v'' + \cdots \\ (c\zeta + c'\zeta' + c''\zeta'' + \cdots)\, z \equiv f\zeta + f'\zeta' + f''\zeta'' + \cdots \\ \cdots\cdots\cdots\cdots, \end{array}$$

die wir der Kürze wegen in folgender Weise darstellen wollen:

$$\Sigma(a\xi)\, x \equiv \Sigma(f\xi), \quad \Sigma(bv)\, y \equiv \Sigma(fv), \quad \Sigma(c\zeta)\, z \equiv \Sigma(f\zeta), \ \ldots$$

4. Nunmehr sind mehrere Fälle zu unterscheiden.

Erstens, wenn sämtliche Coefficienten $\Sigma(a\xi)$, $\Sigma(bv), \ldots$ der Unbekannten zu dem Modul m der Congruenzen prim sind, so lassen sich diese Congruenzen nach den vorher angegebenen Regeln lösen, und die vollständige Lösung des Problems wird dargestellt werden durch Congruenzen von der Form: $x \equiv p \pmod{m}$, $y \equiv q \pmod{m}, \ldots$*).

Sind z. B. die Congruenzen gegeben:

$$x + 3y + z \equiv 1, \quad 4x + y + 5z \equiv 7, \quad 2x + 2y + z \equiv 3 \pmod{8},$$

so findet man $\xi = 9$, $\xi' = 1$, $\xi'' = -14$; hieraus wird $-15x \equiv -26$, daher $x \equiv 6 \pmod{8}$. Auf dieselbe Weise findet man $15y \equiv -4$, $15z \equiv 1$ und hieraus $y \equiv 4$, $z \equiv 7 \pmod{8}$.

5. Zweitens, wenn nicht sämtliche Coefficienten $\Sigma(a\xi)$, $\Sigma(bv), \ldots$ zum Modul prim sind, so seien $\alpha, \beta, \gamma, \ldots$ die grössten gemeinschaftlichen Teiler von m und $\Sigma(a\xi)$, $\Sigma(bv)$, $\Sigma(c\zeta), \ldots$ respective. Offenbar ist dann die Aufgabe unmöglich, wofern nicht jene auch zugleich Teiler der Zahlen $\Sigma(f\xi)$, $\Sigma(fv)$, $\Sigma(f\zeta), \ldots$ respective sind. Wenn aber diese Bedingungen stattfinden, so werden die Congruenzen in (3) durch solche von den Formen $x \equiv p$

---

*) Es mag bemerkt werden, dass dieser Schluss eines Beweises bedarf, den wir aber hier unterdrücken. Denn eigentlich folgt aus unserer Deduction nichts weiter, als dass die gegebenen Congruenzen durch andere Werte der Unbekannten $x, y, z, \ldots$ nicht gelöst werden können; dass diese aber genügen, folgt nicht. Möglicherweise nämlich könnte es gar keine Lösung geben. Ein ähnlicher Paralogismus wird auch in der Theorie der linearen Gleichungen häufig begangen.

$\left(\text{mod.}\ \frac{m}{\alpha}\right)$, $y \equiv q \left(\text{mod.}\ \frac{m}{\beta}\right)$, $z \equiv r \left(\text{mod.}\ \frac{m}{\gamma}\right)$, ... vollständig gelöst werden, oder es wird, wenn man lieber will, α verschiedene $\Big($d. i. nach dem Modul m incongruente, wie p, $p + \frac{m}{\alpha}$, .., $p + \frac{(\alpha - 1)\,m}{\alpha}\Big)$ Werte von x, β verschiedene Werte von y, u. s. w. geben, welche jenen Congruenzen genügen; und offenbar werden alle Lösungen der gegebenen Congruenzen (wenn es deren überhaupt giebt) unter jenen enthalten sein. Indessen darf man diesen Schluss nicht umkehren; denn in den meisten Fällen werden nicht alle Combinationen aller α Werte von x mit allen Werten von y und allen Werten von z u. s. w. der Aufgabe genügen, sondern nur einige von ihnen, deren Zusammenhang man durch eine oder mehrere Bedingungscongruenzen darstellen kann. Da aber die vollständige Lösung dieses Problems für das folgende nicht notwendig ist, so führen wir hier diesen Gegenstand nicht weiter durch, sondern begnügen uns, durch ein **Beispiel** einen Begriff davon zu geben.

Die gegebenen Congruenzen seien:

$$3x + 5y + z \equiv 4,\quad 2x + 3y + 2z \equiv 7,\quad 5x + y + 3z \equiv 6 \ (\text{mod. } 12).$$

Hier werden die Zahlen ξ, ξ', ξ''; v, v', v''; ζ, ζ', ζ'' respective gleich $1, -2, 1$; $1, 1, -1$; $-13, 22, -1$, und aus diesen folgt: $4x \equiv -4$, $7y \equiv 5$, $28z \equiv 96$. Hieraus ergeben sich vier Werte von x, nämlich $x \equiv 2, 5, 8, 11$, ein Wert von y, nämlich $y \equiv 11$, vier Werte von z, nämlich $z \equiv 0, 3, 6, 9$ (mod. 12). Um nun zu wissen, welche Combinationen der Werte von x mit den Werten von z man nehmen darf, substituieren wir in den gegebenen Congruenzen für x, y, z respective $2 + 3t$, 11, $3u$, wodurch dieselben übergehen in die folgenden:

$$57 + 9t + 3u \equiv 0,\quad 30 + 6t + 6u \equiv 0,\quad 15 + 15t + 9u \equiv 0 \ (\text{mod.} 12),$$

und diesen sind, wie man leicht sieht, die folgenden äquivalent:

$$19 + 3t + u \equiv 0,\quad 10 + 2t + 2u \equiv 0,\quad 5 + 5t + 3u \equiv 0 \ (\text{mod. } 4).$$

Die erste erfordert offenbar, dass $u \equiv t + 1$ (mod. 4) sei; setzt man diesen Wert in die beiden andern Congruenzen ein, so findet man, dass auch diesen dadurch genügt wird. Hieraus folgt, dass die folgenden Werte von x: 2, 5, 8, 11 (welche sich ergeben, wenn man $t = 0, 1, 2, 3$ setzt) notwendig mit den folgenden Werten von z respective $z \equiv 3, 6, 9, 0$ combiniert werden müssen, so dass man überhaupt vier Lösungen erhält, nämlich:

$$\begin{aligned} x &\equiv 2,\quad 5,\quad 8,\quad 11 \ (\text{mod. } 12) \\ y &\equiv 11,\ 11,\ 11,\ 11 \\ z &\equiv 3,\quad 6,\quad 9,\quad 0. \end{aligned}$$

Diesen Untersuchungen, durch welche der Zweck des Abschnittes bereits erreicht ist, fügen wir noch einige auf ähnliche Prinzipien sich stützende Sätze hinzu, die wir im Folgenden häufig gebrauchen werden.

Verschiedene Sätze.

38.

Aufgabe. Man soll finden, wieviel positive Zahlen es giebt, die kleiner als eine gegebene positive Zahl A und zugleich prim zu ihr sind.

Bezeichnen wir die Anzahl der positiven Zahlen, welche kleiner als eine gegebene Zahl und zugleich prim zu ihr sind, durch den vor die Zahl gesetzten Buchstaben φ, so wird $\varphi(A)$ gesucht.

I. Ist A eine Primzahl, so sind offenbar alle Zahlen von 1 bis $A-1$ prim zu A; daher ist in diesem Falle:

$$\varphi(A) = A - 1.$$

II. Ist A eine Potenz einer Primzahl, etwa $= p^m$, so werden alle Zahlen mit Ausnahme der durch p teilbaren prim zu A sein. Daher sind von den $p^m - 1$ Zahlen die folgenden wegzulassen: p, $2p$, $3p$, ..., $(p^{m-1} - 1)p$; es bleiben also $p^m - 1 - (p^{m-1} - 1)$ oder $p^{m-1}(p-1)$ Zahlen übrig, so dass ist:

$$\varphi(p^m) = p^{m-1}(p-1).$$

III. Die übrigen Fälle lassen sich leicht auf diese zurückführen mit Hülfe des folgenden **Satzes**:

Ist A in zu einander prime Factoren $M, N, P, \ldots$ zerlegt, so ist

$$\varphi(A) = \varphi(M).\varphi(N).\varphi(P).\ \ldots$$

Derselbe wird folgendermassen bewiesen. Es seien $m, m', m'', \ldots$ die Zahlen, welche prim zu M und kleiner als M sind und deren Anzahl somit $\varphi(M)$ ist. Ebenso seien $n, n', n'', \ldots$ resp. $p, p', p'', \ldots$ die Zahlen, welche prim zu N resp. P und kleiner als N resp. P sind und deren Anzahl gleich $\varphi(N)$ resp. $\varphi(P)$ ist, u. s. w. Nun sind bekanntlich alle zum Producte A primen Zahlen auch zu den einzelnen Factoren $M, N, P, \ldots$ prim und umgekehrt (Artikel 19). Ferner sind alle Zahlen, welche irgend einer der Zahlen $m, m', m'', \ldots$ nach dem Modul M congruent sind, prim zu M und umgekehrt; und dasselbe gilt bezüglich $N, P, \ldots$ Demnach ist die Aufgabe auf die folgende zurückgeführt: Zu bestimmen, wieviel Zahlen es unterhalb A giebt, welche irgend einer der Zahlen $m, m', m'', \ldots$ nach dem Modul M, irgend einer der Zahlen $n, n', n'', \ldots$ nach dem Modul N u. s. w. congruent sind. Aus Artikel 32 folgt aber, dass alle Zahlen, welche nach den einzelnen Moduln $M, N, P, \ldots$ bestimmte Reste geben, nach deren Producte A congruent sind und dass es daher unterhalb A nur eine einzige Zahl giebt, welche nach den einzelnen Zahlen $M, N, P, \ldots$ gegebenen Resten congruent ist. Demnach wird die gesuchte Zahl der Anzahl der Combinationen der einzelnen Zahlen $m, m', m'', \ldots$ mit den einzelnen Zahlen $n, n', n'', \ldots$ und den einzelnen Zahlen $p, p', p'', \ldots$ u. s. w. gleich

sein. Diese Anzahl ist aber, wie aus der Combinationslehre bekannt, gleich $\varphi(M).\ \varphi(N).\ \varphi(P)\ \ldots$

IV. Nun sieht man leicht, wie dies auf den betrachteten Fall anwendbar ist. Zerlegt man A in seine Primfactoren oder bringt man A auf die Form $a^\alpha b^\beta c^\gamma \ldots$, wo $a, b, c, \ldots$ von einander verschiedene Primzahlen bezeichnen, so ist:

$$\varphi(A) = \varphi(a^\alpha).\ \varphi(b^\beta).\ \varphi(c^\gamma) \cdots = a^{\alpha-1}(a-1).\ b^{\beta-1}(b-1).\ c^{\gamma-1}(c-1)\ldots,$$

oder kürzer:

$$\varphi(A) = A\,\frac{a-1}{a}\cdot\frac{b-1}{b}\cdot\frac{c-1}{c}\cdots$$

Beispiel. Ist $A = 60 = 2^2 \cdot 3 \cdot 5$, so ist $\varphi(A) = \frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5}\cdot 60 = 16$. Diese zu 60 primen Zahlen sind: 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59.

Die erste Lösung dieses Problems tritt auf in der Abhandlung Euler's *Theoremata arithmetica nova methodo demonstrata* in den *Comm. nov. Ac. Petrop. VIII p. 74.* Der Beweis ist später in einer andern Abhandlung: *Speculationes circa quasdam insignes proprietates numerorum, Acta Petrop. VIII p. 17,* wiederholt.

39.

Wird die Bedeutung des Functionszeichens φ in solcher Weise bestimmt, dass $\varphi(A)$ die Anzahl der Zahlen, welche prim zu A und nicht grösser als A sind, ausdrücken solle, so ist ersichtlich, dass $\varphi(1)$ nicht mehr gleich 0, sondern gleich 1 ist, und dass hierdurch in allen andern Fällen nichts geändert wird. Nehmen wir diese Definition an, so erhalten wir folgenden **Satz:**

Wenn $a, a', a'', \ldots$ sämtliche Teiler von A (1 und A selbst nicht ausgeschlossen) darstellen, so ist

$$\varphi(a) + \varphi(a') + \varphi(a'') + \ldots = A.$$

Beispiel. Ist $A = 30$, so ist: $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(5) + \varphi(6) + \varphi(10) + \varphi(15) + \varphi(30) = 1 + 1 + 2 + 4 + 2 + 4 + 8 + 8 = 30$.

Beweis. Multipliciert man sämtliche Zahlen, welche prim zu a und nicht grösser als a sind, mit $\frac{A}{a}$, ebenso alle zu a' primen Zahlen mit $\frac{A}{a'}$ u. s. w., so erhält man $\varphi(a) + \varphi(a') + \varphi(a'') + \cdots$ Zahlen, die alle nicht grösser als A sind. Aber

1. alle diese Zahlen sind von einander verschieden. Dass nämlich alle diejenigen Zahlen, welche aus demselben Teiler von A hervorgegangen sind, einander ungleich sind, ist an und für sich klar. Wenn aber aus verschiedenen Teilern M, N, und zu ihnen respective primen Zahlen μ, ν gleiche Zahlen hervorgegangen wären, d. h. wenn $\frac{A}{M}\mu = \frac{A}{N}\nu$ wäre, so müsste $\mu N = \nu M$ sein. Nimmt man nun (was erlaubt ist) $M > N$ an, so müsste M, da es

prim zu μ und ein Teiler von μN ist, auch ein Teiler von N, also die grössere Zahl ein Teiler der kleineren sein, was absurd ist.

2. unter diesen Zahlen kommen die Zahlen $1, 2, 3, \ldots, A$ sämtlich vor. Ist nämlich t eine beliebige A nicht übersteigende Zahl und δ das grösste gemeinschaftliche Mass der Zahlen A und t, so ist $\frac{A}{\delta}$ ein Teiler von A, zu welchem $\frac{t}{\delta}$ prim ist. Offenbar wird daher die Zahl t unter denjenigen vorkommen, welche aus dem Teiler $\frac{A}{\delta}$ hervorgegangen sind.

3. Hieraus folgt, dass die Anzahl aller dieser Zahlen gleich A ist. Daher:

$$\varphi(a) + \varphi(a') + \varphi(a'') + \cdots = A.$$

40.

Ist μ der grösste gemeinschaftliche Teiler der Zahlen $A, B, C, D, \ldots$, so kann man Zahlen $a, b, c, d, \ldots$ von der Beschaffenheit bestimmen, dass

$$aA + bB + cC + \cdots = \mu$$

ist.

Beweis. Betrachten wir zuerst nur zwei Zahlen A, B, und ist λ der grösste gemeinschaftliche Teiler derselben, so ist die Congruenz $Ax \equiv \lambda$ (mod. B) lösbar (Artikel 30). Ist die Wurzel derselben $\equiv \alpha$, und setzt man $\frac{\lambda - A\alpha}{B} = \beta$, so wird: $\alpha A + \beta B = \lambda$, wie verlangt wurde.

Tritt noch eine dritte Zahl C hinzu und ist λ' der grösste gemeinschaftliche Teiler von λ und C, so bestimme man zwei Zahlen k und γ derart, dass $k\lambda + \gamma C = \lambda'$ ist. Dann wird: $k\alpha A + k\beta B + \gamma C = \lambda'$. Offenbar aber ist λ' ein gemeinschaftlicher Teiler von A, B, C, und zwar ist es der grösste, denn gäbe es noch einen grösseren ϑ, so würde der Ausdruck $k\alpha \cdot \frac{A}{\vartheta} + k\beta \cdot \frac{B}{\vartheta} + \gamma \cdot \frac{C}{\vartheta} = \frac{\lambda'}{\vartheta}$ eine ganze Zahl, also die grössere Zahl ϑ ein Teiler der kleineren sein müssen. Das Verlangte ist daher geleistet, wenn man $k\alpha = a$, $k\beta = b$, $\gamma = c$, $\lambda' = \mu$ setzt.

Auf gleiche Weise kann man fortfahren, wie viele andere Zahlen auch immer hinzutreten mögen.

Wenn daher die Zahlen $A, B, C, D \ldots$ keinen gemeinschaftlichen Teiler haben, so kann man offenbar bewirken, dass

$$aA + bB + cC + \cdots = 1$$

wird.

41.

Ist p eine Primzahl und hat man p Dinge, unter denen beliebig viele, nur nicht gerade alle, einander gleich sein können,

so wird die Anzahl der Permutationen dieser Dinge durch p teilbar sein.

Beispiel. Die fünf Gegenstände A, A, A, B, B können auf zehn verschiedene Arten versetzt werden.

Der Beweis dieses Satzes kann leicht aus der bekannten Theorie der Permutationen abgeleitet werden. Denn giebt es unter diesen Gegenständen a, welche gleich A, sodann b, welche gleich B, ferner c, welche gleich C u. s. w. sind (wo die Zahlen a, b, c, ... auch die Einheit bezeichnen können), so dass

$$a + b + c + \cdots = p$$

ist, so ist die Anzahl der Permutationen gleich

$$\frac{1 \cdot 2 \cdot 3 \cdots p}{1 \cdot 2 \cdot 3 \cdots a \cdot 1 \cdot 2 \cdot 3 \cdots b \cdot 1 \cdot 2 \cdot 3 \cdots c \cdots}.$$

Nun ist an und für sich klar, dass der Zähler dieses Bruches durch den Nenner teilbar ist, da die Anzahl der Permutationen eine ganze Zahl sein muss. Der Zähler aber ist teilbar durch p, der Nenner dagegen, welcher aus Factoren, die kleiner als p sind, gebildet ist, ist nicht teilbar durch p (Artikel 15). Demnach ist die Anzahl der Permutationen durch p teilbar (Artikel 19).

Es dürfte jedoch, hoffe ich, manchem der folgende Beweis nicht unwillkommen sein.

Wenn in zwei Permutationen die Ordnung der Gegenstände, aus denen sie gebildet sind, nur in so fern abweicht, dass derjenige Gegenstand, welcher in der einen den ersten Platz einnimmt, in der andern einen andern Platz hat, die übrigen aber in beiden in derselben Reihenfolge fortschreiten und auf den letzten Gegenstand in der einen derjenige folgt, welcher in der andern der erste ist, so nennen wir diese Permutationen ähnliche Permutationen.*) So werden in unserm Beispiele $ABAAB$ und $ABABA$ ähnliche Permutationen sein, weil die Gegenstände, welche in der ersteren den ersten, zweiten u. s. w. Platz einnehmen, in der letzteren an dem dritten, vierten, u. s. w. Platze in derselben Reihenfolge sich befinden.

Da nun jede Permutation aus p Gegenständen besteht, so kann man offenbar zu jeder $p - 1$ ähnliche finden, wenn man denjenigen Gegenstand, welcher der erste gewesen war, an den zweiten, dritten u. s. w. Platz fortrückt. Wenn unter diesen identische sich nicht befinden können, so ist klar, dass die Anzahl aller Permutationen durch p teilbar werden wird, da diese p-mal grösser ist, als die Anzahl aller unähnlichen Permutationen.

---

*) Denkt man sich ähnliche Permutationen in einen Kreis geschrieben, so dass der letzte Gegenstand dem ersten benachbart wird, so wird überhaupt kein Unterschied existieren, da kein Platz der erste oder letzte genannt werden kann.

Wir nehmen daher an, dass zwei Permutationen

$$PQ\ldots TV\ldots YZ,\quad V\ldots YZPQ\ldots T,$$

von denen die eine aus der andern durch das Fortrücken der Glieder entstanden ist, identisch seien oder dass $P = V$ u. s. w. sei. Ist das Glied P, welches in der ersteren das erste ist, in der letzteren das $n+1^{\text{te}}$, so wird also in der letzteren Reihe das $n+1^{\text{te}}$ Glied dem ersten, das $n+2^{\text{te}}$ Glied dem zweiten u. s. w., also das $2n+1^{\text{te}}$ Glied wiederum dem ersten gleich und aus demselben Grunde auch das $3n+1^{\text{te}}$, u. s. w., allgemein das $kn+m^{\text{te}}$ gleich dem m^{ten} (Hierbei ist, sobald $kn+m > p$ ist, entweder die Reihe $V\ldots YZPQ\ldots T$ immer wieder von Anfang an wiederholt zu denken oder von $kn+m$ das nächstkleinere Vielfache von p zu subtrahieren). Wenn daher k so bestimmt wird, dass $kn \equiv 1$ (mod. p) ist, was möglich ist, da p eine Primzahl sein soll, so folgt allgemein, dass das m^{te} Glied dem $m+1^{\text{ten}}$ oder dass jedes Glied dem folgenden gleich ist, d. h. dass alle Glieder einander gleich sind, was gegen die Voraussetzung ist.

42.

Wenn die Coefficienten $A, B, C, \ldots, N$; $a, b, c, \ldots, n$ zweier Functionen von der Form

$$(P)\qquad x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} + \cdots + N$$
$$(Q)\qquad x^\mu + ax^{\mu-1} + bx^{\mu-2} + cx^{\mu-3} + \cdots + n$$

sämtlich rationale, aber nicht sämtlich ganze Zahlen sind und das Product aus (P) und (Q) durch

$$x^{m+\mu} + \mathfrak{A}x^{m+\mu-1} + \mathfrak{B}x^{m+\mu-2} + \cdots + \mathfrak{Z}$$

dargestellt wird, so können die Coefficienten $\mathfrak{A}, \mathfrak{B}, \ldots, \mathfrak{Z}$ nicht sämtlich ganze Zahlen sein.

Beweis. Man drücke alle Brüche unter den Coefficienten $A, B, \ldots$ $a, b, \ldots$ durch die möglich kleinsten Zahlen aus und wähle nach Belieben eine Primzahl p, welche in einem oder mehreren von den Nennern dieser Brüche ohne Rest aufgeht. Nimmt man an, was erlaubt ist, dass p in dem Nenner irgend eines gebrochenen Coefficienten in (P) aufgeht, so wird es offenbar, wenn man (Q) durch p teilt, auch in $\frac{(Q)}{p}$ wenigstens einen gebrochenen Coefficienten geben, dessen Nenner den Factor p enthält $\left(\text{nämlich den ersten Coefficienten } \frac{1}{p}\right)$. Nun sieht man leicht, dass es in P ein Glied, einen Bruch, geben wird, dessen Nenner mehr Dimensionen von p, als die Nenner aller vorhergehenden ähnlichen Glieder, und nicht weniger als die Nenner aller folgenden, besitzt. Dieses Glied sei Gx^g und die Anzahl der

Dimensionen von p im Nenner von G sei t. Ein ähnliches Glied giebt es in $\frac{(Q)}{p}$; dasselbe sei Γx^γ und die Anzahl der Dimensionen von p im Nenner von Γ sei τ. Dann ist offenbar $t+\tau$ mindestens gleich 2. Nach diesen Vorbereitungen wird das Glied $x^{g+\gamma}$ des Products von (P) und (Q) einen gebrochenen Coefficienten haben, dessen Nenner $t+\tau-1$ Dimensionen von p enthält. Dies wird folgendermassen bewiesen.

Es seien $'Gx^{g+1}$, $''Gx^{g+2}$, ... diejenigen Glieder, welche in (P) dem Gliede Gx^g vorangehen, $G'x^{g-1}$, $G''x^{g-2}$, ... aber diejenigen, welche ihm folgen. Ebenso seien $'\Gamma x^{\gamma+1}$, $''\Gamma x^{\gamma+2}$, ... diejenigen Glieder, welche in $\frac{(Q)}{p}$ dem Gliede Γx^γ vorangehen, $\Gamma' x^{\gamma-1}$, $\Gamma'' x^{\gamma-2}$ aber diejenigen, welche ihm folgen. Dann ist offenbar der Coefficient des Gliedes $x^{g+\gamma}$ in dem Producte aus (P) und $\frac{(Q)}{p}$ gleich:

$$\begin{aligned} G\Gamma + {'G}\Gamma' + {''G}\Gamma'' + \cdots \\ + {'\Gamma} G' + {''\Gamma} G'' + \cdots \end{aligned}$$

Der Teil $G\Gamma$ ist ein Bruch, welcher, in den kleinsten Zahlen ausgedrückt, im Nenner $t+\tau$ Dimensionen von p enthält; die übrigen Teile aber enthalten, wenn sie Brüche sind, im Nenner weniger Dimensionen von p, da sie sämtlich Producte aus je zwei Factoren sind, von denen der eine nicht mehr als t, der andere aber weniger als τ Dimensionen von p enthält, oder von denen der eine nicht mehr als τ, der andere aber weniger als t Dimensionen von p besitzt. Demnach ist $G\Gamma$ von der Form $\frac{e}{fp^{t+\tau}}$, während die Summe der übrigen Teile von der Form $\frac{e'}{f'p^{t+\tau-\delta}}$ ist, wo δ eine positive Zahl ist und e, f, f' den Factor p nicht enthalten. Somit ist die Summe aller gleich $\frac{ef'+e'fp^\delta}{ff'p^{t+\tau}}$. Da der Zähler dieses Ausdrucks durch p nicht teilbar ist, so kann der Nenner durch keine Reduction weniger Dimensionen von p erhalten als $t+\tau$. Daher ist der Coefficient des Gliedes $x^{g+\gamma}$ in dem Producte von (P) und (Q) gleich

$$\frac{ef'+e'fp^\delta}{ff'p^{t+\tau-1}}$$

d. h. er ist ein Bruch, dessen Nenner $t+\tau-1$ Dimensionen von p enthält. Damit ist der Satz bewiesen.

43.

Die Congruenz m^{ten} Grades

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \cdots + Mx + N \equiv 0,$$

deren Modul eine in A nicht aufgehende Primzahl p ist, kann nicht auf mehr denn auf m verschiedene Arten gelöst werden oder hat nicht mehr als m nach dem Modul p incongruente Wurzeln (Siehe Artikel 25. 26).

Wäre dies nicht der Fall, so nehmen wir an, dass es Congruenzen verschiedener Grade $m, n, \ldots$ gäbe, welche mehr als $m, n, \ldots$ Wurzeln haben, und es sei m der kleinste Grad, so dass alle ähnlichen Congruenzen der niederen Grade mit unserm Satze in Übereinstimmung sich befinden. Da wir dies für den ersten Grad schon oben (Artikel 26) bewiesen haben, so ist klar, dass m entweder gleich 2 oder grösser als 2 ist. Es besitze also die Congruenz

$$Ax^m + Bx^{m-1} + \cdots + Mx + N \equiv 0$$

wenigstens $m+1$ Wurzeln, welche $x \equiv \alpha$, $x \equiv \beta$, $x \equiv \gamma, \ldots$ sein mögen, und man nehme an, was erlaubt ist, dass alle Zahlen $\alpha, \beta, \gamma, \ldots$ positiv und kleiner als p seien und dass die kleinste von allen α sei. Man substituiere nun in der gegebenen Congruenz $y+\alpha$ für x, wodurch sie übergehen möge in:

$$A'y^m + B'y^{m-1} + C'y^{m-2} + \cdots + M'y + N' \equiv 0.$$

Dann wird offenbar dieser Congruenz genügt werden, wenn man $y \equiv 0$ oder $y \equiv \beta - \alpha$ oder $y \equiv \gamma - \alpha$ u. s. w. setzt, welche Wurzeln alle von einander verschieden sind und deren Anzahl gleich $m+1$ ist. Daraus aber, dass $y \equiv 0$ eine Wurzel ist, folgt, dass N' durch p teilbar ist. Daher ist auch der Ausdruck

$$y(A'y^{m-1} + B'y^{m-2} + \cdots + M') \equiv 0 \pmod{p},$$

wenn man y einen der m Werte $\beta - \alpha, \gamma - \alpha, \ldots$, welche sämtlich grösser als 0 und kleiner als p sind, beilegt, und daher wird in allen diesen Fällen auch

$$A'y^{m-1} + B'y^{m-2} + \cdots + M' \equiv 0 \text{ (Artikel 22)}$$

sein, d. h. die Congruenz

$$A'y^{m-1} + B'y^{m-2} + \cdots + M' \equiv 0,$$

welche vom $m-1^{\text{ten}}$ Grade ist, wird m Wurzeln haben und somit im Widerspruch stehen mit unserem Satze (offenbar nämlich ist $A' = A$ und daher, wie erforderlich, A' nicht teilbar durch p), obwohl wir angenommen haben, dass alle Congruenzen von niedrigerem Grade als dem m^{ten} mit demselben in Übereinstimmung sich befinden. Damit ist der Satz allgemein bewiesen.

44.

Obwohl wir angenommen haben, dass der Modul p im Coefficienten des höchsten Gliedes nicht aufgehen solle, ist doch der Satz auf diesen Fall nicht beschränkt. Wenn nämlich der erste Coefficient oder auch einige der folgenden durch p teilbar wären, so könnte man diese Glieder ruhig weg-

lassen und dadurch schliesslich die Congruenz auf eine von niedrigerem Grade zurückführen, bei welcher der erste Coefficient nicht mehr durch p teilbar wäre, es müssten denn gerade alle Coefficienten durch p teilbar sein, in welchem Falle die Congruenz eine identische und die Unbekannte völlig unbestimmt sein würde.

Dieser Satz wurde zuerst von Lagrange aufgestellt und bewiesen *(Mém. de l'Ac. de Berlin, Année 1768 p. 192).* Er kommt auch vor in einer Abhandlung von Legendre, *Recherches d'Analyse indéterminée, Hist. de l'Ac. de Paris 1785 p. 466.* Euler bewies in den *Nov. Comm. Ac. Petrop. XVIII p. 93,* dass die Congruenz $x^n - 1 \equiv 0$ mehr wie n verschiedene Wurzeln nicht haben könne. Obwohl dieselbe nur ein specieller Fall ist, ist die Methode, deren er sich bediente, auf alle Congruenzen leicht anwendbar. Einen noch specielleren Fall hatte er schon vorher in den *Comm. nov. Ac. Petrop. V. p. 6* absolviert, aber die hierbei gebrauchte Methode lässt sich nicht allgemein anwenden. Unten im Abschnitt VIII werden wir den Satz noch auf eine andere Art beweisen: aber wie verschieden auch beim ersten Anblick alle diese Methoden erscheinen könnten, so würden doch Kundige, die sie vergleichen wollten, sich leicht überzeugen, dass sie alle auf demselben Princip aufgebaut sind. Da übrigens dieser Satz hier nur gleichsam als Hülfssatz zu betrachten ist und eine vollständige Auseinandersetzung hier nicht hergehört, so überheben wir uns der Mühe, zusammengesetzte Moduln noch besonders zu behandeln.

Dritter Abschnitt.

Von den Potenzresten.

Die Reste der Glieder einer mit der Einheit anfangenden geometrischen Reihe bilden eine periodische Reihe.

45.

Satz. In jeder geometrischen Progression $1, a, a^2, a^3, \ldots$ giebt es ausser dem ersten Gliede 1 noch ein anderes der Einheit nach dem zu a primen Modul p congruentes Glied a^t, dessen Exponent $t < p$ ist.

Beweis. Da der Modul p zu a und somit auch zu jeder beliebigen Potenz von a prim ist, so ist kein Glied der Progression $\equiv 0 \pmod{p}$, sondern vielmehr ein jedes irgend einer der Zahlen $1, 2, 3, \ldots, p-1$ congruent. Da die Anzahl dieser Zahlen gleich $p-1$ ist, so können offenbar, wenn mehr als $p-1$ Glieder der Progression in Betracht gezogen werden, diese nicht sämtlich verschiedene kleinste Reste haben. Demnach befinden sich unter den Gliedern $1, a, a^2, a^3, \ldots, a^{p-1}$ mindestens zwei congruente. Es sei also $a^m \equiv a^n$ und $m > n$; dann wird, wenn man durch a^n dividiert, $a^{m-n} \equiv 1$ (Artikel 22), wo $m - n < p$ und > 0 ist.

Beispiel. So findet man in der Progression $2, 4, 8, \ldots$ als erstes Glied, welches nach dem Modul 13 der Einheit congruent ist, das Glied $2^{12} = 4096$. In derselben Progression ist nach dem Modul $23: 2^{11} = 2048 \equiv 1$. Ebenso ist die sechste Potenz der Zahl 5, d. i. 15625, nach dem Modul 7, dagegen die fünfte, 3125, nach dem Modul 11 der Einheit congruent. In einigen Fällen also wird schon eine Potenz mit kleinerem Exponenten als $p-1$ der Einheit congruent, in andern dagegen muss man bis zur $p-1^{\text{ten}}$ Potenz aufsteigen.

46.

Wird die Progression über das Glied hinaus, welches der Einheit congruent ist, fortgesetzt, so gehen dieselben Reste, welche man im Anfang hatte, wiederum hervor. Ist nämlich $a^t \equiv 1$, so wird $a^{t+1} \equiv a$, $a^{t+2} \equiv a^2$, u. s. w., bis man zu dem Gliede a^{2t} gelangt, dessen kleinster Rest wiederum

$\equiv 1$ ist, und die **Periode** der Reste beginnt von Neuem. Man erhält daher eine t Reste umfassende Periode, welche, nachdem sie zu Ende ist, immer von Anfang an sich wiederholt; und es können in der ganzen Progression keine andern Reste vorkommen, als die, welche in dieser Periode enthalten sind. Allgemein ist $a^{mt} \equiv 1$ und $a^{mt+n} \equiv a^n$, was wir in unserer Bezeichnung so darstellen:

Ist $r \equiv \rho$ (mod. t), so ist auch $a^r \equiv a^\rho$ (mod. p).

47.

Aus diesem Satze ergiebt sich ein einfaches Verfahren, die Reste von Potenzen mit beliebig hohem Exponenten aufzufinden, sobald man weiss, welche Potenz der Einheit congruent ist. Sucht man z. B. den Rest, welcher bei der Division der Potenz 3^{1000} durch 13 übrig bleibt, so ist, wegen $3^3 \equiv 1$ (mod. 13), $t = 3$. Da nun $1000 \equiv 1$ (mod. 3), ist, so ist $3^{1000} \equiv 3$ (mod. 13).

48.

Ist a^t die niedrigste Potenz, welche der Einheit congruent ist (ausser $a^0 = 1$, auf welchen Fall wir hier keine Rücksicht nehmen), so werden jene t Glieder, welche die Periode der Reste bilden, sämtlich verschieden sein, wie man aus dem Beweise des Artikels 45 ohne Mühe erkennt. Dann kann aber der Satz des Artikels 46 umgekehrt werden, nämlich: Ist $a^m \equiv a^n$ (mod. p), so ist $m \equiv n$ (mod. t). Denn wenn m, n nach dem Modul t incongruent wären, so würden ihre kleinsten Reste verschieden sein. Nun ist aber $a^\mu \equiv a^m$, $a^\nu \equiv a^n$, daher $a^\mu \equiv a^\nu$, d. h. nicht alle Potenzen unterhalb a^t würden incongruent sein, was gegen die Voraussetzung ist.

Wenn daher $a^k \equiv 1$ (mod. p) ist, so ist $k \equiv 0$ (mod. t), d. h. k ist durch t teilbar.

Bisher haben wir von beliebigen Moduln, wofern sie nur zu a prim sind, gesprochen. Jetzt wollen wir die Moduln, welche absolute Primzahlen sind, gesondert betrachten und auf diesem Grunde nachher die allgemeinere Untersuchung aufbauen.

Es werden zunächst Moduln, welche Primzahlen sind, betrachtet.

49.

Satz. Ist p eine Primzahl, welche in a nicht aufgeht, und ist a^t die niedrigste Potenz von a, welche nach dem Modul p der Einheit congruent ist, so ist der Exponent t entweder gleich $p - 1$ oder ein aliquoter Teil dieser Zahl.

Man vergleiche die Beispiele im Artikel 45.

Beweis. Da wir bereits gezeigt haben, dass t entweder $= p-1$ oder $< p-1$ ist, so bleibt nur übrig uns davon zu überzeugen, dass im letzteren Falle t immer ein aliquoter Teil von $p-1$ ist.

I. Man nehme die kleinsten positiven Reste aller dieser Glieder $1, a, a^2, \ldots, a^{t-1}$ und bezeichne dieselben durch $\alpha, \alpha', \alpha'', \ldots$, so dass $\alpha = 1$, $\alpha' \equiv a$, $\alpha'' \equiv a^2, \ldots$ ist. Offenbar sind alle diese verschieden, denn wenn zwei Glieder a^m, a^n dieselben Reste liessen, so würde (unter der Annahme $m > n$) $a^{m-n} \equiv 1$ und $m - n < t$ sein, was absurd ist, da nach Voraussetzung keine niedrigere Potenz als a^t der Einheit congruent ist. Ferner sind alle Zahlen $\alpha, \alpha', \alpha'', \ldots$ in der Reihe der Zahlen $1, 2, 3, \ldots, p-1$ enthalten, doch werden sie dieselbe nicht ganz erschöpfen, da $t < p-1$ ist. Den Complex aller Zahlen $\alpha, \alpha', \alpha'', \ldots$ werden wir durch (A) bezeichnen. Es wird also (A) t Glieder umfassen.

II. Man nehme nun aus der Reihe der Zahlen $1, 2, 3, \ldots, p-1$ irgend eine β, welche in dem Complex (A) fehlt, multipliciere β mit allen Zahlen $\alpha, \alpha', \alpha'', \ldots$ und bezeichne die daraus entstehenden kleinsten Reste mit $\beta, \beta', \beta'', \ldots$, deren Anzahl dann ebenfalls gleich t ist. Diese Reste werden aber sowohl unter sich als von allen den Zahlen $\alpha, \alpha', \alpha'', \ldots$ verschieden sein. Wäre nämlich die erste Behauptung nicht richtig, so hätte man etwa $\beta a^m \equiv \beta a^n$ und daher, nach Division durch β, $a^m \equiv a^n$, was mit dem eben Bewiesenen im Widerspruch steht; wäre aber die zweite Behauptung falsch, so hätte man etwa $\beta a^m \equiv a^n$ und daher, unter der Annahme, dass $m < n$ ist, $\beta \equiv a^{n-m}$, d. h. es würde β irgend einer der Zahlen $\alpha, \alpha', \alpha'', \ldots$ congruent sein, was gegen die Voraussetzung ist. Ist jedoch $m > n$, so folgt, nach Multiplikation mit a^{t-m}, $\beta a^t \equiv a^{t+n-m}$ oder, da $a^t \equiv 1$ ist, $\beta \equiv a^{t+n-m}$, was aus demselben Grunde absurd ist. Bezeichnet man den Complex aller Zahlen $\beta, \beta', \beta'', \ldots$, deren Anzahl gleich t ist, mit (B), so hat man in beiden Complexen (A) und (B) aus der Reihe $1, 2, 3, \ldots, p-1$ bereits $2t$ Zahlen. Wenn daher (A) und (B) alle diese Zahlen umfassen, so ist $\frac{p-1}{2} = t$, und der Satz ist bewiesen.

III. Fehlen aber noch einige, so sei eine von diesen gleich γ. Mit dieser multipliciere man sämtliche Zahlen $\alpha, \alpha', \alpha'', \ldots$, bezeichne die kleinsten Reste der Producte mit $\gamma, \gamma', \gamma'', \ldots$ und den Complex aller dieser mit (C). Dann wird also (C) t Zahlen der Reihe $1, 2, 3, \ldots, p-1$ enthalten, und diese werden sowohl unter sich als von den in (A) und (B) enthaltenen Zahlen verschieden sein. Die beiden ersten Behauptungen werden auf dieselbe Weise wie in II., die dritte folgendermassen bewiesen: Wäre $\gamma a^m \equiv \beta a^n$, so würde entweder $\gamma \equiv \beta a^{n-m}$ oder $\gamma \equiv \beta a^{t+n-m}$ sein, je nachdem $m < n$ oder $m > n$ wäre; in jedem Falle würde also γ entgegen der Voraussetzung irgend einer im Complex (B) enthaltenen Zahl congruent sein. Man hat daher $3t$ Zahlen aus der Reihe $1, 2, 3, \ldots, p-1$, und wenn keine weiter fehlen, so wird $t = \frac{p-1}{3}$ und daher der Satz bewiesen sein.

IV. Wenn aber immer noch welche fehlen, so muss man in derselben Weise zu einem vierten Complex (D) von Zahlen weitergehen. Da aber die Anzahl der Zahlen $1, 2, 3, \ldots, p-1$ eine endliche ist, so muss dieselbe offenbar einmal erschöpft werden und daher ein Vielfaches von t sein. Somit ist t ein aliquoter Teil von $p-1$.

Der Fermat'sche Satz.

50.

Da also $\frac{p-1}{t}$ eine ganze Zahl ist, so folgt, wenn man beide Seiten der Congruenz $a^t \equiv 1$ zur $\frac{p-1}{t}$ten Potenz erhebt, $a^{p-1} \equiv 1$, oder: Die Differenz $a^{p-1}-1$ ist stets durch p teilbar, wenn p eine in a nicht aufgehende Primzahl ist.

Dieser Satz, welcher sowohl wegen seiner Eleganz als wegen seines hervorragenden Nutzens höchst beachtenswert ist, wird gewöhnlich nach seinem Erfinder das Fermat'sche Theorem genannt. Siehe *Fermatii Opera Mathematica, Tolosae 1679, p. 163.* Einen Beweis fügt der Erfinder nicht hinzu, doch behauptet er, im Besitze eines solchen zu sein. Euler veröffentlichte zuerst einen Beweis in der Abhandlung: *Theorematum quorundam ad numeros primos spectantium demonstratio, Comm. Acad. Petrop. T. VIII.**) Derselbe stützt sich auf die Entwicklung der Potenz $(a+1)^p$, bei der man aus der Form der Coefficienten sehr leicht herleitet, dass stets $(a+1)^p - a^p - 1$ durch p teilbar ist und daher auch $(a+1)^p - (a+1)$ durch p sich teilen lässt, falls $a^p - a$ durch p teilbar ist. Da nun $1^p - 1$ stets durch p teilbar ist, so ist es auch $2^p - 2$, demnach auch $3^p - 3$ u. s. w. und allgemein $a^p - a$. Wenn daher p in a nicht aufgeht, so wird auch $a^{p-1} - 1$ durch p teilbar sein. — Dies wird genügen, um das Wesen der Methode klarzulegen. Einen ähnlichen Beweis hat Lambert in den *Acta Erudit. 1769 p. 109* angegeben. Da jedoch die Entwicklung der Potenz eines Binoms der Theorie der Zahlen ziemlich fremdartig zu sein schien, hat Euler einen anderen Beweis gesucht, der in den *Comment. nov. Petrop. T. VII p. 70* zu finden ist und mit dem von uns im vorhergehenden Artikel gegebenen völlig übereinstimmt. Im Folgenden werden sich uns noch einige

*) In einer früheren Abhandlung war er noch nicht zum Ziele gelangt. *Comm. Ac. Petr. T. VI p. 106.* — In dem berüchtigten Streite zwischen Maupertuis und König, der wegen des Prinzips der kleinsten Aktion entstanden war, aber bald zu andern Sachen überging, behauptet König im Besitze eines Briefes von Leibnitz zu sein, in dem ein mit dem Euler'schen vollkommen übereinstimmender Beweis enthalten sei. *Appel au public, p. 106.* Wenn wir auch die Glaubwürdigkeit dieses Zeugnisses nicht in Zweifel ziehen wollen, so hat doch sicher Leibnitz seine Erfindung nie veröffentlicht. Vgl. *Hist. de l'Ac. de Berlin, Année 1750 p. 530.*

andere darbieten. An dieser Stelle wollen wir noch einen anfügen, der sich auf ähnliche Principien stützt, wie der erste von Euler. Der folgende Satz, von welchem unser Satz nur ein besonderer Fall ist, wird unten auch bei anderen Untersuchungen Anwendung finden.

51.

Die p^{te} Potenz des Polynoms $a+b+c+\cdots$ ist dem Ausdruck $a^p+b^p+c^p+\cdots$ nach dem Modul p congruent, falls p eine Primzahl ist.

Beweis. Bekanntlich wird die p^{te} Potenz des Polynoms $a+b+c+\cdots$ gebildet aus Gliedern von der Form $\varkappa a^\alpha b^\beta c^\gamma \ldots$, wo $\alpha+\beta+\gamma+\cdots=p$ ist und die Zahl $\varkappa$ angiebt, auf wie viel Arten p Gegenstände, von denen $\alpha, \beta, \gamma, \ldots$ respective gleich $a, b, c, \ldots$ sind, permutiert werden können. Wir haben aber oben im Artikel 41 gezeigt, dass diese Zahl immer durch p teilbar ist, wenn nicht alle Gegenstände gleich sind, d. i. wenn nicht irgend eine der Zahlen $\alpha, \beta, \gamma, \ldots$ gleich p, die übrigen aber gleich 0 sind. Hieraus folgt, dass alle Glieder von $(a+b+c+\cdots)^p$ mit Ausnahme von $a^p, b^p, c^p, \ldots$ durch p teilbar sind. Dieselben können also, sobald es sich um eine Congruenz nach dem Modul p handelt, ganz weggelassen werden, und es wird:

$$(a+b+c+\cdots)^p \equiv a^p+b^p+c^p+\cdots$$

Werden nun sämtliche Grössen $a, b, c, \ldots$ gleich 1 gesetzt und ihre Anzahl gleich k, so wird $k^p \equiv k$, wie im vorigen Artikel.

Über die Anzahl der Zahlen, denen Perioden entsprechen, in welchen die Anzahl der Glieder ein gegebener Teiler von $p-1$ ist.

52.

Da somit keine andern Zahlen als diejenigen, welche Teiler von $p-1$ sind, Exponenten der kleinsten Potenzen, zu welchen irgend welche Zahlen erhoben werden müssen, um der Einheit congruent zu werden, sein können, so entsteht die Frage, ob alle Teiler von $p-1$ hierzu sich eignen, und ferner, wenn sämtliche durch p nicht teilbare Zahlen nach dem Exponenten ihrer niedrigsten, der Einheit congruenten Potenz in Klassen geteilt werden, wie viele Zahlen auf die einzelnen Exponenten kommen werden. Hierbei kann man sogleich bemerken, dass es ausreicht, wenn alle positiven Zahlen von 1 bis $p-1$ in Betracht gezogen werden. Denn offenbar müssen congruente Zahlen, um der Einheit congruent zu werden, auf dieselbe Potenz erhoben werden, und daher ist jede Zahl auf denselben Exponenten wie ihr kleinster positiver Rest zu beziehen. Wir müssen daher unsere Aufmerksamkeit darauf richten, zu ermitteln, wie nach diesem Gesichtspunkte die Zahlen $1, 2, 3, \ldots, p-1$ unter die einzelnen Factoren von $p-1$ zu ver-

teilen sind. Der Kürze wegen wollen wir, wenn d einer der Teiler von $p-1$ (zu denen auch 1 und $p-1$ zu rechnen sind) ist, mit $\psi(d)$ die Anzahl der positiven unterhalb p gelegenen Zahlen bezeichnen, deren d^{te} Potenz die niedrigste ist, welche der Einheit congruent ist.

53.

Damit diese Untersuchung leichter verständlich werde, setzen wir ein **Beispiel** her. Für $p = 19$ werden sich die Zahlen 1, 2, 3, ..., 18 unter die Teiler der Zahl 18 in folgender Weise verteilen:

1	1.					
2	18.					
3	7.	11.				
6	8.	12.				
9	4.	5.	6.	9.	16.	17.
18	2.	3.	10.	13.	14.	15.

In diesem Falle wird also $\psi(1) = 1$, $\psi(2) = 1$, $\psi(3) = 2$, $\psi(6) = 2$, $\psi(9) = 6$, $\psi(18) = 6$. Eine geringe Aufmerksamkeit zeigt hierbei, dass ebenso viele Zahlen zu jedem Exponenten gehören, als es Zahlen giebt, die nicht grösser als er und prim zu ihm sind, oder dass wenigstens in diesem Falle, mit Beibehaltung der Bezeichnung im Artikel 39, $\psi(d) = \varphi(d)$ ist. Dass aber diese Bemerkung allgemein gültig sei, können wir folgendermassen beweisen.

I. Hat man irgend eine Zahl a, welche zum Exponenten d **gehört** (d. h. deren d^{te} Potenz der Einheit congruent ist, während alle niedrigeren Potenzen derselben nicht congruent sind), so werden alle Potenzen derselben $a^2, a^3, a^4, \ldots, a^d$ oder deren kleinste Reste erstere Eigenschaft (nämlich dass die d^{te} Potenz derselben der Einheit congruent ist) ebenfalls besitzen und da dies auch so ausgedrückt werden kann, dass die kleinsten Reste der Zahlen $a, a^2, a^3, \ldots, a^d$ (welche sämtlich von einander verschieden sind) Wurzeln der Congruenz $x^d \equiv 1$ sind, diese Congruenz aber mehr als d verschiedene Wurzeln nicht haben kann, so ist klar, dass es ausser den kleinsten Resten der Zahlen $a, a^2, a^3, \ldots, a^d$ andere Zahlen zwischen 1 und $p-1$ incl. nicht giebt, deren d^{te} Potenzen der Einheit congruent sind. Hieraus geht hervor, dass sich alle zum Exponenten d gehörige Zahlen unter den kleinsten Resten der Zahlen $a, a^2, a^3, \ldots, a^d$ vorfinden. Welcher Art dieselben aber sind und wie gross ihre Anzahl ist, lässt sich so bestimmen: Ist k eine zu d prime Zahl, so werden sämtliche Potenzen von a^k, deren Exponenten kleiner als d sind, der Einheit nicht congruent sein. Denn es sei $\frac{1}{k} \pmod{d} \equiv m$ (siehe Artikel 31), so ist: $a^{km} \equiv a$; wenn daher die e^{te} Potenz von a^k der Einheit congruent und $e < d$ wäre, so würde auch $a^{kme} \equiv 1$ und daher gegen die Voraussetzung $a^e \equiv 1$ sein. Hieraus erhellt,

dass der kleinste Rest von a^k zum Exponenten d gehört. — Wenn aber k mit d irgend einen gemeinschaftlichen Teiler δ hat, so gehört der kleinste Rest von a^k nicht zum Exponenten d, weil ja alsdann schon die $\frac{d}{\delta}$te Potenz der Einheit congruent ist (es wird nämlich $\frac{kd}{\delta}$ durch d teilbar oder $\equiv 0$ (mod. d) und daher $a^{\frac{kd}{\delta}} \equiv 1$ sein). Hieraus folgt, dass zum Exponenten d soviele Zahlen gehören, als es unter den Zahlen $1, 2, 3, \ldots, d$ relative Primzahlen zu d giebt. Man muss aber im Gedächtnis behalten, dass dieser Schluss sich auf die Annahme stützt, dass man bereits eine zum Exponenten d gehörige Zahl a habe. Daher bleibt die Möglichkeit offen, dass zu irgend einem Exponenten überhaupt gar keine Zahl gehört, und unser Schluss ist dahin zu beschränken, dass $\psi(d)$ entweder $= 0$ oder $= \varphi(d)$ ist.

54.

II. Sind nun $d, d', d'', \ldots$ sämtliche Teiler von $p-1$, so ist, weil alle Zahlen $1, 2, 3, \ldots, p-1$ unter dieselben verteilt sind:

$$\psi(d) + \psi(d') + \psi(d'') + \cdots = p - 1.$$

In Artikel 40 haben wir aber bewiesen, dass

$$\varphi(d) + \varphi(d') + \varphi(d'') + \cdots = p - 1$$

ist, und aus dem vorhergehenden Artikel folgt, dass $\psi(d)$ entweder gleich $\varphi(d)$ oder kleiner, aber nicht grösser als $\varphi(d)$ sein könne, und dasselbe gilt von $\psi(d')$ und $\varphi(d')$ u. s. w. Wenn daher irgend ein (oder mehrere) Glied der Reihe $\psi(d), \psi(d'), \psi(d''), \ldots$ kleiner als das entsprechende Glied der Reihe $\varphi(d), \varphi(d'), \varphi(d''), \ldots$ wäre, so würde die Summe jener der Summe dieser nicht gleich sein können. Hieraus schliessen wir endlich, dass $\psi(d)$ stets gleich $\varphi(d)$ ist und somit von der Grösse von $p-1$ nicht abhängt.

55.

Die grösste Beachtung aber verdient ein besonderer Fall des vorigen Satzes, nämlich dass es immer Zahlen giebt, deren niedrigste Potenz, welche der Einheit congruent ist, die $p-1$te ist, und zwar ebenso viele zwischen 1 und $p-1$, als es unterhalb $p-1$ zu $p-1$ prime Zahlen giebt. Da der Beewis dieses Satzes keineswegs so auf der Hand liegt, als es auf den ersten Anblick scheinen könnte, so wollen wir wegen der Bedeutung des Satzes noch einen andern von dem vorigen etwas verschiedenen Beweis anfügen, zumal die Verschiedenheit der Methoden gewöhnlich sehr viel zur Erläuterung etwas schwerer verständlicher Dinge beiträgt. Man zerlege $p-1$ in seine Primfactoren, und zwar sei $p-1 = a^\alpha b^\beta c^\gamma \ldots$, wo $a, b, c, \ldots$ ungleiche Primzahlen bedeuten. Alsdann können wir den Beweis des Satzes in folgender Weise durchführen:

I. Es lässt sich immer eine (oder mehrere) Zahl A finden, welche zum Exponenten a^α gehört, und ebenso Zahlen $B, C, \ldots$, welche respective zu den Exponenten b^β, c^γ, ... gehören.

II. Das Product aller Zahlen $A, B, C, \ldots$ (oder der kleinste Rest dieses Products) gehört zum Exponenten $p-1$.

Dies beweisen wir folgendermassen.

I. Ist g irgend eine der Zahlen $1, 2, 3, \ldots, p-1$, welche der Congruenz $x^{\frac{p-1}{a}} \equiv 1 \pmod{p}$ nicht genügt, da nicht alle diese Zahlen dieser Congruenz, deren Grad kleiner als $p-1$ ist, genügen können, so behaupte ich, dass, wenn die $\frac{p-1}{a^\alpha}$te Potenz von g congruent h gesetzt wird, diese Zahl oder ihr kleinster Rest zum Exponenten a^α gehört.

Denn offenbar wird die a^αte Potenz von h der $p-1$ten Potenz von g d. i. der Einheit congruent sein, während die $a^{\alpha-1}$te Potenz von h der $\frac{p-1}{a}$ Potenz von g congruent d. i. der Einheit nicht congruent ist; und um so weniger können die $a^{\alpha-2}$, $a^{\alpha-3}$ten u. s. w. Potenzen von h der Einheit congruent sein. Der Exponent der kleinsten der Einheit congruenten Potenz von h oder der Exponent, zu welchem h gehört, muss aber (nach Artikel 48) in der Zahl a^α aufgehen. Mithin muss notwendig, da a^α durch keine anderen Zahlen als durch sich selbst und durch niedrigere Potenzen von a teilbar ist, a^α der Exponent sein, zu welchem h gehört. Auf analoge Weise zeigt man, dass es Zahlen giebt, die zu den Exponenten b^β, c^γ, ... gehören.

II. Nehmen wir an, dass das Product aus allen Zahlen $A, B, C, \ldots$ nicht zum Exponenten $p-1$, sondern zu einem niedrigeren t gehöre, so wird t in $p-1$ aufgehen (Artikel 48), oder es wird $\frac{p-1}{t}$ eine ganze die Einheit übersteigende Zahl sein. Man sieht aber leicht, dass dieser Quotient entweder eine der Primzahlen $a, b, c, \ldots$, oder wenigstens durch irgend eine derselben, z. B. durch a, da bezüglich der andern der Beweis derselbe bleibt, teilbar ist (Artikel 17). Es wird daher t in $\frac{p-1}{a}$ aufgehen und somit wird auch das Product $ABC\ldots$ auf die $\frac{p-1}{a}$te Potenz erhoben der Einheit congruent sein (Artikel 46). Es ist aber klar, dass die einzelnen Zahlen $B, C, \ldots$ (ausser A), auf die $\frac{p-1}{a}$te Potenz erhoben, der Einheit congruent werden, da die Exponenten b^β, c^γ, ..., zu welchen die einzelnen gehören, in $\frac{p-1}{a}$ aufgehen. Daher wird sein:

$$A^{\frac{p-1}{a}} B^{\frac{p-1}{a}} C^{\frac{p-1}{a}} \ldots \equiv A^{\frac{p-1}{a}} \equiv 1.$$

Hieraus folgt, dass der Exponent, zu welchem A gehört, ein Teiler von $\frac{p-1}{a}$ (Artikel 48) d. i. $\frac{p-1}{a^{\alpha+1}}$ eine ganze Zahl sein muss. Nun kann aber $\frac{p-1}{a^{\alpha+1}} = \frac{b^\beta c^\gamma \ldots}{a}$ keine ganze Zahl sein (Artikel 15); somit müssen wir endlich schliessen, dass unsere Annahme nicht richtig sein kann, dass vielmehr das Product $ABC \ldots$ wirklich zum Exponenten $p-1$ gehört.

Der letztere Beweis scheint etwas weitläufiger als der erste, dieser aber dafür weniger direct zu sein als jener.

56.

Dieser Satz liefert ein ausgezeichnetes Beispiel dafür, wie grosse Vorsicht oft in der Theorie der Zahlen erforderlich ist, damit man nicht das für ausgemacht annehme, was es in Wirklichkeit nicht ist, Lambert erwähnt in seiner schon oben angeführten Abhandlung, *Acta Erudit. 1769 p. 127,* diesen Satz, ohne auch nur von der Notwendigkeit eines Beweises zu reden. Niemand aber hat den Beweis versucht ausser Euler: *Comment. nov. Ac. Petrop. T. XVIII für das Jahr 1773, Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia p. 85 u. ff.* Man sehe besonders Artikel 37, wo er sich über die Notwendigkeit eines Beweises weitläufiger auslässt. Doch leidet der Beweis, welchen der scharfsinnige Autor giebt, an zwei Mängeln. Der eine besteht darin, dass er im Artikel 31 u. ff. stillschweigend annimmt, dass die Congruenz $x^n \equiv 1$ (mit Übertragung der dort angewandten Redeweise in unsere Bezeichnung) wirklich n verschiedene Wurzeln habe, obwohl vorher nur bewiesen worden ist, dass sie nicht mehr als n Wurzeln haben kann; der andere ist der, dass er die Formel des Artikels 34 nur durch Induction abgeleitet hat.

Primitive Wurzeln, Grundzahlen, Indices.

57.

Die zum Exponenten $p-1$ gehörigen Zahlen werden wir mit Euler **primitive Wurzeln** nennen. Wenn also a eine primitive Wurzel ist, so werden die kleinsten Reste der Potenzen $a, a^2, a^3, \ldots, a^{p-1}$ sämtlich von einander verschieden sein, woraus sich leicht ergiebt, dass sich unter diesen alle Zahlen $1, 2, 3, \ldots, p-1$, deren Anzahl ebenso gross ist, wie die jener kleinsten Reste, vorfinden müssen, d. h. dass jede durch p nicht teilbare Zahl irgend einer Potenz von a congruent ist. Diese ausgezeichnete Eigenschaft ist von dem grössten Nutzen und kann die arithmetischen, auf die Congruenzen bezüglichen Operationen sehr erheblich erleichtern, etwa in derselben Weise, wie die Einführung der Logarithmen die Operationen der gemeinen Arithmetik. Wir werden nach Belieben irgend eine

primitive Wurzel a als **Basis** oder **Grundzahl** annehmen und auf diese alle durch p nicht teilbaren Zahlen beziehen, und wenn $a^e \equiv b$ (mod. p) ist, so werden wir e den **Index** von b nennen. Wenn z. B. für den Modul 19 die primitive Wurzel 2 als Basis genommen wird, so werden

den Zahlen	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.	18.
die Indices	0.	1.	13.	2.	16.	14.	6.	3.	8.	17.	12.	15.	5.	7.	11.	4.	10.	9

entsprechen. Übrigens ist klar, dass, wenn die Basis dieselbe bleibt, einer jeden Zahl mehrere Indices zukommen, dass aber diese sämtlich nach dem Modul $p-1$ congruent sind. So oft daher von den Indices die Rede sein wird, werden diejenigen, welche nach dem Modul $p-1$ congruent sind, als äquivalent betrachtet werden, ähnlich wie die Zahlen selbst, wenn sie nach dem Modul p congruent sind, als äquivalent gelten.

Algorithmus der Indices.

58.

Die auf die Indices bezüglichen Sätze sind durchaus analog denen, welche für die Logarithmen gelten.

Der Index des Products aus beliebig vielen Factoren ist der Summe der Indices der einzelnen Factoren nach dem Modul $p-1$ congruent.

Der Index der Potenz irgend einer Zahl ist dem Producte aus dem Index der gegebenen Zahl und dem Exponenten der Potenz nach dem Modul $p-1$ congruent.

Die Beweise lassen wir ihrer Leichtigkeit halber weg.

Hieraus ist ersichtlich, dass, wenn man eine Tafel construieren wollte, aus der man die Indices aller Zahlen für verschiedene Moduln entnehmen könnte, aus derselben sowohl alle Zahlen, welche grösser als der Modul sind, als auch alle zusammengesetzten Zahlen fortgelassen werden könnten. Eine Probe einer solchen Tafel ist am Schlusse dieses Werkes als Tafel I angefügt. Auf derselben stehen in der ersten Vertikalreihe die Primzahlen und deren Potenzen von 3 bis 97, die als Moduln zu betrachten sind, neben jeder von ihnen die zur Basis genommenen Zahlen; dann folgen die Indices der aufeinanderfolgenden Primzahlen, von denen immer je fünf durch einen kleinen Zwischenraum getrennt sind; in derselben Weise sind am Kopfe der Tafel die Primzahlen angeordnet, so dass man leicht und sicher finden kann, welcher Index einer gegebenen Primzahl nach einem gegebenen Modul entspricht.

Ist z. B. $p = 67$ so ist der Index der Zahl 60, wenn man 12 zur Basis nimmt:

$$\equiv 2 \text{ ind. } 2 + \text{ind. } 3 + \text{ind. } 5 \text{ (mod. } 66) \equiv 58 + 9 + 39 \equiv 40.$$

59.

Der Index jedes Wertes des Ausdrucks $\frac{a}{b}$ (mod. p) (Artikel 31) ist nach dem Modul $p-1$ der Differenz der Indices des Zählers a und des Nenners b congruent, wofern die Zahlen a und b durch p nicht teilbar sind.

Ist nämlich c irgend ein Wert des Ausdrucks, so ist $bc \equiv a$ (mod. p), daher:

$$\text{ind.}\, b + \text{ind.}\, c \equiv \text{ind.}\, a \ (\text{mod.}\, p-1)$$

und somit

$$\text{ind.}\, c \equiv \text{ind.}\, a - \text{ind.}\, b.$$

Wenn man daher eine Tafel hat, aus welcher der einer jeden Zahl nach jedem beliebigen Primzahlmodul entsprechende Index, und eine andere, aus welcher die zu einem gegebenen Index gehörige Zahl entnommen werden kann, so lassen sich sämtliche Congruenzen ersten Grades mit der grössten Leichtigkeit lösen, da man alle auf solche zurückführen kann, deren Modul eine Primzahl ist (Artikel 30). Ist z. B. die Congruenz $29x + 7 \equiv 0$ (mod. 47) vorgelegt, so wird: $x \equiv \frac{-7}{29}$ (mod. 47), also:

$$\text{ind.}\, x \equiv \text{ind.}\, (-7) - \text{ind.}\, 29 \equiv \text{ind.}\, 40 - \text{ind.}\, 29 \equiv 15 - 43 \equiv 18 \ (\text{mod.}\, 46).$$

Der Index 18 aber gehört zur Zahl 3. Demnach ist $x \equiv 3$ (mod. 47). Eine zweite Tafel haben wir allerdings nicht hinzugefügt, doch kann an Stelle dieser eine andere dienen, wie wir im sechsten Abschnitt zeigen werden.

Über die Wurzeln der Congruenz $x^n \equiv A$.

60.

In analoger Weise, wie wir im Artikel 31 die Wurzeln der Congruenzen ersten Grades bezeichnet haben, werden wir im Folgenden auch die Wurzeln der reinen Congruenzen höherer Grade durch ein Zeichen darstellen. Wie nämlich $\sqrt[n]{A}$ nichts anderes bedeutet als eine Wurzel der Gleichung $x^n = A$, so wird mit Hinzufügung des Moduls durch $\sqrt[n]{A}$ (mod. p) jede beliebige Wurzel der Congruenz $x^n \equiv A$ (mod. p) bezeichnet werden. Wir werden sagen, dass dieser Ausdruck $\sqrt[n]{A}$ (mod. p) so viele Werte besitze, als er nach dem Modul p incongruente Werte hat, da sämtliche nach p congruente Werte als äquivalent zu betrachten sind (Artikel 26). Überdies ist klar, dass, wenn A und B nach dem Modul p congruent waren, die Ausdrücke $\sqrt[n]{A}$ (mod. p) und $\sqrt[n]{B}$ (mod. p) einander äquivalent sein werden.

Setzt man nun $\sqrt[n]{A} \equiv x$ (mod. p), so wird n ind. $x \equiv$ ind. A (mod. $p-1$). Aus dieser Congruenz ergeben sich nach den Regeln des vorigen

Abschnitts die Werte von ind. x und aus diesen die entsprechenden Werte von x. Man sieht aber leicht, dass x soviele Werte besitzt, als die Congruenz n ind. $x \equiv$ ind. A (mod. $p-1$) Wurzeln hat. Offenbar also wird $\sqrt[n]{A}$ nur einen Wert haben, wenn n zu $p-1$ prim ist; wenn aber die Zahlen n und $p-1$ einen gemeinschaftlichen Teiler δ haben und dieser der grösste ist, so wird ind. x δ nach dem Modul $p-1$ incongruente Werte und daher $\sqrt[n]{A}$ ebensoviele nach dem Modul p incongruente Werte haben, wofern ind. A durch δ teilbar ist. Ist diese Bedingung nicht erfüllt, so wird $\sqrt[n]{A}$ keinen reellen Wert besitzen.

Beispiel. Man sucht die Werte des Ausdrucks $\sqrt[15]{11}$ (mod. 19). Dann muss man also die Congruenz 15 ind. $x \equiv$ ind. $11 \equiv 6$ (mod. 18) lösen, und findet dadurch die drei Werte ind. $x \equiv 4$, 10, 16 (mod. 18). Diesen entsprechen aber die Werte $x \equiv 6$, 9, 4 (mod. 19).

61.

So einfach auch diese Methode ist, wenn man die nötigen Tafeln zur Hand hat, so dürfen wir doch nicht vergessen, dass sie eine indirecte ist. Es wird daher der Mühe wert sein, zu untersuchen, wieviel directe Methoden vermögen, und zwar werden wir hier das anführen, was sich aus dem Vorhergehenden folgern lässt, dagegen das andere, welches tiefere Betrachtungen erfordert, für den achten Abschnitt vorbehalten. Wir beginnen mit dem einfachsten Fall, in welchem $A = 1$ ist, wo also die Wurzeln der Congruenz $x^n \equiv 1$ (mod. p) gesucht werden. Hier muss somit, wenn eine beliebige primitive Wurzel zur Basis genommen wird, n ind. $x \equiv 0$ (mod. $p-1$) sein. Diese Congruenz wird, wenn n zu $p-1$ prim ist, nur eine einzige Wurzel haben, nämlich ind. $x \equiv 0$ (mod. $p-1$), daher hat in diesem Falle $\sqrt[n]{1}$ (mod. p) einen einzigen Wert, nämlich $\equiv 1$. Wenn aber die Zahlen n und $p-1$ den (grössten) gemeinschaftlichen Teiler δ haben, so wird die vollständige Lösung der Congruenz n ind. $x \equiv 0$ (mod. $p-1$) sein: ind. $x \equiv 0 \left(\text{mod. } \frac{p-1}{\delta}\right)$ (Siehe Artikel 29), d. h. es wird ind. x nach dem Modul $p-1$ irgend einer der Zahlen

$$0,\ \frac{p-1}{\delta},\ \frac{2(p-1)}{\delta},\ \frac{3(p-1)}{\delta},\ldots,\ \frac{(\delta-1)(p-1)}{\delta}$$

congruent sein müssen oder δ nach dem Modul $p-1$ incongruente Werte besitzen; daher wird auch x in diesem Falle δ verschiedene (nach dem Modul p incongruente) Werte haben. Hieraus ist ersichtlich, dass der Ausdruck $\sqrt[\delta]{1}$ ebenfalls δ verschiedene Werte hat, deren Indices mit den vorher angegebenen Zahlen völlig übereinstimmen. Daher ist der Ausdruck $\sqrt[\delta]{1}$ (mod. p) dem Ausdruck $\sqrt[n]{1}$ (mod. p) durchaus äquivalent, d. h. die

Congruenz $x^\delta \equiv 1 \pmod{p}$ hat dieselben Wurzeln wie $x^n \equiv 1 \pmod{p}$. Die erstere aber wird von niedrigerem Grade sein als letztere, wofern δ und n ungleich sind.

Beispiel. $\sqrt[15]{1} \pmod{19}$ hat drei Werte, weil 3 der grösste gemeinschaftliche Teiler der Zahlen 15 und 18 ist, und diese werden zu gleicher Zeit die Werte von $\sqrt[3]{1} \pmod{19}$ sein. Diese sind aber 1, 7, 11.

62.

Durch diese Reduction gewinnen wir also den Vorteil, dass wir keine andern Congruenzen von der Form $x^n \equiv 1$ zu lösen brauchen, als solche, in denen n ein Teiler von $p-1$ ist. Weiter unten werden wir aber zeigen, dass sich die Congruenzen von dieser Form immer noch weiter erniedrigen lassen, doch reicht hierzu das Vorhergehende nicht aus. Nur einen Fall können wir schon hier erledigen, nämlich den, wo $n = 2$ ist. Offenbar nämlich sind $+1$ und -1 die Werte des Ausdrucks $\sqrt[2]{1}$, da er mehr wie zwei nicht haben kann und $+1$ und -1 immer incongruent sind, wofern nicht der Modul gleich 2 ist, in welchem Falle es an sich klar ist, dass $\sqrt[n]{1}$ nur einen Wert haben kann. Hieraus folgt, dass $+1$ und -1 auch die Werte des Ausdrucks $\sqrt[2m]{1}$ sein werden, falls m zu $\frac{p-1}{2}$ prim ist. Dies ist immer der Fall, so oft der Modul derart ist, dass $\frac{p-1}{2}$ eine absolute Primzahl ist (es müsste denn gerade $p-1 = 2m$ sein, in welchem Falle alle Zahlen $1, 2, 3, \ldots, p-1$ Wurzeln sind), z. B. wenn $p = 3, 5, 7, 11, 23, 47, 59, 83, 107, \ldots$ ist. Als Corollar mag hier hinzugefügt werden, dass der Index von -1 immer $\equiv \frac{p-1}{2} \pmod{p-1}$ ist, welche primitive Wurzel man auch zur Basis nehmen möge. Denn es ist: $2 \text{ ind. } (-1) \equiv 0 \pmod{p-1}$; daher ist ind. (-1) entweder $\equiv 0$ oder $\equiv \frac{p-1}{2} \pmod{p-1}$. Es ist aber 0 immer der Index von $+1$ und $+1$ und -1 müssen stets verschiedene Indices haben (ausser im Falle $p = 2$, auf den wir hier erst keine Rücksicht zu nehmen brauchen).

63.

Im Artikel 60 haben wir gezeigt, dass der Ausdruck $\sqrt[n]{A} \pmod{p}$ entweder δ verschiedene Werte oder gar keinen Wert besitzt, wenn δ der grösste gemeinschaftliche Teiler der Zahlen n und $p-1$ ist. Wie wir nun eben $\sqrt[n]{A}$ und $\sqrt[\delta]{A}$ als äquivalent nachgewiesen haben, wenn $A \equiv 1$ ist, so werden wir jetzt allgemeiner beweisen, dass der Ausdruck $\sqrt[n]{A}$ immer auf einen andern $\sqrt[\delta]{B}$ reduciert werden kann, dem er äquivalent ist. Bezeichnet man nämlich irgend einen Wert jenes Ausdrucks durch x, so wird $x^n \equiv A$.

Ist nun t irgend ein Wert des Ausdrucks $\frac{\delta}{n}$ (mod. $p-1$), der, wie aus Artikel 31 ersichtlich ist, reelle Werte besitzt, so wird $x^{nt} \equiv A^t$. Es ist aber $x^{nt} \equiv x^\delta$ wegen $tn \equiv \delta$ (mod. $p-1$). Somit ist $x^\delta \equiv A^t$, und daher wird jeder beliebige Wert von $\sqrt[n]{A}$ auch ein Wert von $\sqrt[\delta]{A^t}$ sein. So oft also der Ausdruck $\sqrt[n]{A}$ reelle Werte hat, wird er dem Ausdruck $\sqrt[\delta]{A^t}$ völlig äquivalent sein, da jener weder andere noch weniger Werte hat als dieser, obwohl es geschehen kann, dass, wenn $\sqrt[n]{A}$ keinen reellen Wert hat, doch $\sqrt[\delta]{A^t}$ reelle Werte besitzt.

Beispiel. Werden die Werte des Ausdrucks $\sqrt[21]{2}$ (mod. 31) gesucht, so ist der grösste den Zahlen 21 und 30 gemeinschaftliche Teiler gleich 3 und irgend ein Wert des Ausdrucks $\frac{3}{21}$ (mod. 30) ebenfalls gleich 3. Besitzt daher der Ausdruck $\sqrt[21]{2}$ reelle Werte, so wird er dem Ausdruck $\sqrt[3]{2^3}$ oder $\sqrt[3]{8}$ äquivalent sein, und in der That findet man, dass die Werte des letzteren Ausdrucks, nämlich 2, 10, 19, auch dem ersteren genügen.

64.

Damit wir aber nicht Gefahr laufen, diese Operation vergeblich unternommen zu haben, müssen wir eine Regel ermitteln, nach welcher man sogleich beurteilen kann, ob $\sqrt[n]{A}$ reelle Werte zulässt oder nicht. Hat man eine Tafel der Indices zur Hand, so ist die Sache klar; denn aus Artikel 60 geht hervor, dass es reelle Werte giebt oder nicht, je nachdem der Index von A für irgend eine zur Basis genommene primitive Wurzel durch δ teilbar ist oder nicht. Dies kann jedoch auch ohne Hülfe einer solchen Tafel gefunden werden. Setzt man nämlich den Index von A gleich k, so wird, wenn dieser durch δ teilbar ist, $\frac{k(p-1)}{\delta}$ durch $p-1$ teilbar sein und umgekehrt. Nun ist aber der Index der Zahl $A^{\frac{p-1}{\delta}}$ gleich $\frac{k(p-1)}{\delta}$. Wenn daher $\sqrt[n]{A}$ (mod. p) reelle Werte hat, so wird $A^{\frac{p-1}{\delta}}$ der Einheit congruent sein, im andern Falle dagegen nicht. So hat man in dem Beispiel des vorigen Artikels $2^{10} = 1024 \equiv 1$ (mod. 31), woraus folgt, dass $\sqrt[21]{2}$ (mod. 31) reelle Werte hat. Ebenso erhalten wir hieraus die Überzeugung, dass $\sqrt[2]{-1}$ (mod. p) stets zwei reelle Werte hat, wenn p von der Form $4m+1$, dagegen keinen, wenn p von der Form $4m+3$ ist, da $(-1)^{2m} = 1$ und $(-1)^{2m+1} = -1$ ist. Dieser elegante **Satz**, welcher gewöhnlich in folgender Form ausgesprochen wird: Ist p eine Primzahl von der Form $4m+1$, so kann man immer eine Quadratzahl a^2 von solcher Beschaffenheit finden, dass a^2+1 durch p teilbar wird; ist aber p eine Primzahl von der Form $4m-1$, so giebt es eine solche Quadrat-

zahl nicht — ist in dieser Weise von Euler in den *Comm. nov. Acad. Petrop. T. XVIII p. 112 für das Jahr 1773* bewiesen worden. Einen andern Beweis hatte er schon viel früher gegeben in den *Comm. nov. T. V p. 5*, welcher Band 1760 erschien. In einer früheren Abhandlung in den *Comm. nov. T. IV p. 25* war er damit noch nicht zu Stande gekommen. Später hat dann auch Lagrange in den *Nouveaux Mém. de l'Ac. de Berlin, A. 1775 p. 342* einen Beweis des Satzes gegeben. Noch einen andern Beweis werden wir im folgenden Abschnitte, wo im Specielleren über diesen Gegenstand gehandelt werden wird, bringen.

65.

Nachdem wir alle Ausdrücke $\sqrt[n]{A}$ (mod. p) auf solche zurückzuführen gelehrt haben, wo n ein Teiler der Zahl $p-1$ ist, und zugleich ein Kriterium dafür erlangt haben, zu entscheiden, ob sie reelle Werte besitzen oder nicht, wollen wir jetzt derartige Ausdrücke $\sqrt[n]{A}$ (mod. p), in denen n ein Teiler von $p-1$ ist, etwas genauer betrachten. Zuerst werden wir zeigen, welche Beziehung die einzelnen Werte des Ausdrucks zu einander haben, sodann werden wir gewisse Kunstgriffe angeben, mittelst deren man sehr häufig einen Wert des Ausdrucks finden kann.

Erstens, wenn $A \equiv 1$ und r irgend einer der n Werte des Ausdrucks $\sqrt[n]{1}$ (mod. p) oder $r^n \equiv 1$ (mod. p) ist, so werden auch sämtliche Potenzen von r Werte jenes Ausdrucks sein; von diesen aber werden so viel von einander verschieden sein, als der Exponent, zu welchem r gehört, Einheiten hat (Art. 48). Ist daher r der zum Exponenten n gehörige Wert, so werden die Potenzen desselben $r, r^2, r^3, \ldots, r^n$ (wo man für den letzten auch die Einheit setzen kann) sämtliche Werte des Ausdrucks $\sqrt[n]{1}$ (mod. p) umfassen. Welche Hülfsmittel aber existieren, um solche Werte, welche zum Exponenten n gehören, zu finden, werden wir im achten Abschnitt ausführlicher auseinandersetzen.

Zweitens, wenn A der Einheit nicht congruent und ein Wert des Ausdrucks $\sqrt[n]{A}$ (mod. p), welcher z heissen möge, bekannt ist, so kann man daraus die übrigen in folgender Weise finden. Sind (wie wir eben gezeigt haben)

$$1,\ r,\ r^2,\ \ldots,\ r^{n-1}$$

sämtliche Werte von $\sqrt[n]{1}$, so werden

$$z,\ zr,\ zr^2,\ \ldots,\ zr^{n-1}$$

sämtliche Werte des Ausdrucks $\sqrt[n]{A}$ sein. Denn dass alle diese Werte der Congruenz $x^n \equiv A$ genügen, geht daraus hervor, dass, wenn man irgend einen derselben $\equiv zr^k$ setzt, die n^{te} Potenz davon, nämlich $z^n r^{nk}$, wegen $r^n \equiv 1$ und $z^n \equiv A$, congruent A wird, und dass alle diese Werte ver-

schieden sind, ist aus Artikel 23 leicht ersichtlich. Mehr Werte aber als diese, deren Anzahl gleich n ist, kann der Ausdruck $\sqrt[n]{A}$ nicht haben. So wird z. B., wenn der eine Wert des Ausdrucks $\sqrt[2]{A}$ gleich z ist, der andere gleich $-z$ sein. Schliesslich muss man hieraus folgern, dass man nicht alle Werte des Ausdrucks $\sqrt[n]{A}$ finden kann, wenn nicht zugleich sämtliche Werte des Ausdrucks $\sqrt[n]{1}$ bekannt sind.

66.

Das zweite, was wir uns vorgenommen hatten, war zu zeigen, in welchem Falle ein Wert des Ausdrucks $\sqrt[n]{A}$ (mod. p) (wo n als Divisor von $p-1$ vorausgesetzt ist) direct gefunden werden kann. Dies ist der Fall, wenn irgend ein Wert irgend einer Potenz von A congruent wird, und da dieser Fall nicht selten eintritt, wird es nicht überflüssig sein, ein wenig bei dieser Sache zu verweilen. Es sei, wenn es überhaupt einen giebt, z ein solcher Wert oder $z \equiv A^k$ und $A \equiv z^n$ (mod. p). Hieraus folgt $A \equiv A^{kn}$. Hat man daher eine Zahl k von solcher Beschaffenheit, dass $A \equiv A^{kn}$ ist, so wird A^k der gesuchte Wert sein. Dieser Bedingung ist aber die folgende äquivalent, dass $1 \equiv kn$ (mod. t) sein soll, wo t den Exponenten, zu welchem A gehört, bezeichnet (Artikel 46, 48). Damit aber diese Congruenz möglich sei, ist erforderlich, dass n prim zu t sei. In diesem Falle wird $k \equiv \frac{1}{n}$ (mod. t); haben aber t und n einen gemeinschaftlichen Teiler, so kann kein Wert z einer Potenz von A congruent sein.

67.

Da wir aber für diese Lösung t selbst kennen müssen, wollen wir sehen, wie wir verfahren können, wenn diese Zahl nicht bekannt ist. Zuerst ist leicht ersichtlich, dass t in $\frac{p-1}{n}$ aufgehen muss, wofern $\sqrt[n]{A}$ (mod. p) reelle Werte hat, wie wir hier immer voraussetzen. Ist nämlich ein beliebiger Wert dieses Ausdrucks gleich y, so ist sowohl $y^{p-1} \equiv 1$, als auch $y^n \equiv A$ (mod. p). Erhebt man daher beide Seiten der letzteren Congruenz auf die $\frac{p-1}{n}$te Potenz, so wird $A^{\frac{p-1}{n}} \equiv 1$, und daher muss $\frac{p-1}{n}$ durch t teilbar sein (Artikel 48). Wenn nun $\frac{p-1}{n}$ zu n prim ist, so lässt sich die Congruenz im vorigen Artikel, nämlich $kn \equiv 1$, auch nach dem Modul $\frac{p-1}{n}$ lösen, und der der Congruenz nach diesem Modul genügende Wert von k wird offenbar derselben Congruenz auch nach dem Modul t, welcher in $\frac{p-1}{n}$ aufgeht, genügen (Artikel 5). Dann ist also das, was gesucht wurde, ge-

funden. — Ist aber $\frac{p-1}{n}$ nicht prim zu n, so werfe man alle Primfactoren von $\frac{p-1}{n}$, welche zugleich in n aufgehen, aus $\frac{p-1}{n}$ heraus. Dadurch erhalten wir eine zu n prime Zahl $\frac{p-1}{nq}$, wo q das Product aus allen jenen Primfactoren, die wir fortgeworfen haben, bezeichnet. Wenn nun die Bedingung, zu welcher wir im vorigen Artikel gelangt sind, nämlich dass t zu n prim sei, stattfindet, so wird auch t prim zu q sein und daher auch in $\frac{p-1}{nq}$ aufgehen. Löst man also die Congruenz $kn \equiv 1 \left(\text{mod. } \frac{p-1}{nq}\right)$ (was möglich ist, weil n zu $\frac{p-1}{nq}$ prim ist), so wird der Wert von k der Congruenz auch nach dem Modul t genügen, was verlangt wurde. Dieser ganze Kunstgriff besteht darin, eine Zahl zu ermitteln, welche die Stelle von t, das wir nicht kennen, vertreten kann. Jedoch muss man wohl im Gedächtnis behalten, dass wir, im Falle $\frac{p-1}{n}$ zu n nicht prim ist, angenommen haben, dass die Bedingung des vorigen Artikels erfüllt ist. Ist dies nicht der Fall, so sind alle Schlüsse irrig; und wenn man beim unachtsamen Befolgen der gegebenen Regeln einen Wert von z findet, dessen n^{te} Potenz der Zahl A nicht congruent ist, so ist dies ein Zeichen, dass die Bedingung nicht erfüllt ist und daher diese Methode überhaupt nicht angewendet werden kann.

68.

Aber auch in diesem Falle kann es oft von Vorteil sein, sich die Mühe gemacht zu haben, und es verlohnt sich zu untersuchen, wie sich dieser falsche Wert zu dem richtigen verhält. Wir wollen also annehmen, dass k, z der Regel nach bestimmt seien, dass aber z^n nicht $\equiv A$ (mod. p) sei. Wofern wir nur die Werte des Ausdrucks $\sqrt[n]{\frac{A}{z^n}}$ (mod. p) bestimmen können, werden wir dann, indem wir jeden einzelnen mit z multiplicieren, Werte von $\sqrt[n]{A}$ erhalten. Ist nämlich v irgend ein Werth von $\sqrt[n]{\frac{A}{z^n}}$, so wird $(vz)^n \equiv A$. Der Ausdruck $\sqrt[n]{\frac{A}{z^n}}$ ist aber insofern einfacher als $\sqrt[n]{A}$, weil $\frac{A}{z^n}$ (mod. p) meistens zu einem kleineren Exponenten gehört, als A. Wenn nämlich d der grösste gemeinschaftliche Teiler von t und q ist, so wird $\frac{A}{z^n}$ (mod. p) zum Exponenten d gehören, was folgendermassen bewiesen wird. Substituiert man für z seinen Wert, so wird $\frac{A}{z^n} \equiv \frac{1}{A^{kn-1}}$ (mod. p).

Nun ist aber $kn-1$ durch $\frac{p-1}{nq}$ teilbar (nach vorigem Artikel), dagegen $\frac{p-1}{n}$ durch t (ebenda) oder $\frac{p-1}{nd}$ durch $\frac{t}{d}$. Ferner ist $\frac{t}{d}$ prim zu $\frac{q}{d}$ (nach Voraussetzung) und somit auch $\frac{p-1}{nd}$ durch $\frac{tq}{d^2}$ oder $\frac{p-1}{nq}$ durch $\frac{t}{d}$, also auch $kn-1$ durch $\frac{t}{d}$ und $(kn-1)\,d$ durch t teilbar. Hieraus folgt: $A^{(kn-1)d} \equiv 1$ (mod. p), woraus man leicht ableitet, dass $\frac{A}{z^n}$ zur d^{ten} Potenz erhoben der Einheit congruent wird. Dass aber $\frac{A}{z^n}$ nicht zu einem kleineren Exponenten als d gehören kann, lässt sich zwar leicht beweisen, doch halten wir uns, da dies für unsern Zweck nicht erforderlich ist, damit nicht auf. Wir können also sicher sein, dass $\frac{A}{z^n}$ (mod. p) stets zu einem kleineren Exponenten gehört als A, einen einzigen Fall ausgenommen, nämlich wenn t in q aufgeht und daher $d = t$ ist.

Doch was nützt es, dass $\frac{A}{z^n}$ zu einem kleineren Exponenten gehört, als A? Es giebt mehr Zahlen, die A sein können, als solche, die $\frac{A}{z^n}$ sein können, und wenn wir mehrere solche Ausdrücke wie $\sqrt[n]{A}$ nach demselben Modul entwickeln sollen, haben wir den Vorteil, dass wir mehrere aus einer und derselben Quelle ableiten können. So werden wir z. B. stets wenigstens einen Wert des Ausdrucks $\sqrt[2]{A}$ (mod. 29) zu bestimmen imstande sein, wofern nur die Werte von $\sqrt[2]{-1}$ (mod. 29) (welche ± 12 sind) bekannt sind. Denn aus dem vorigen Artikel ist leicht ersichtlich, dass ein Wert derartiger Ausdrücke immer direct bestimmt werden kann, wenn t ungerade ist, und dass $d = 2$ wird, wenn t gerade ist; ausser -1 aber gehört keine Zahl zum Exponenten 2.

Beispiele. Man sucht die Werte von $\sqrt[3]{31}$ (mod. 37). Hier ist $p-1 = 36$, $n = 3$, $\frac{p-1}{3} = 12$ und daher $q = 3$. Es muss daher $3k \equiv 1$ (mod. 4) sein, und dies ist der Fall, wenn man $k = 3$ setzt. Hieraus ergiebt sich $z \equiv 31^3$ (mod. 37) $\equiv 6$, und in der That findet man: $6^3 \equiv 31$ (mod. 37). Wenn die Werte des Ausdrucks $\sqrt[3]{1}$ (mod. 37) bekannt sind, lassen sich auch die übrigen Werte von $\sqrt[3]{6}$ bestimmen. Jene sind aber 1, 10, 26, und multipliciert man 6 mit diesen, so erhält man die übrigen Werte $\equiv 23$ und 8.

Wenn aber der Wert des Ausdrucks $\sqrt[2]{3}$ (mod. 37) gesucht wird, so ist $n = 2$, $\frac{p-1}{n} = 18$ und daher $q = 2$. Hiernach muss sein $2k \equiv 1$ (mod. 9) und somit $k \equiv 5$ (mod. 9). Daher ist $z \equiv 3^5 \equiv 21$ (mod. 37). Aber 21^2 ist

nicht $\equiv 3$, sondern $\equiv 34$. Es ist jedoch $\frac{3}{34}$ (mod. 37) $\equiv -1$ und $\sqrt[2]{-1}$ (mod. 37) $\equiv \pm 6$. Hieraus erhält man die richtigen Werte $\pm 6 \cdot 21 \equiv \pm 15$.

Dies ist ungefähr das, was wir hier über die Entwicklung derartiger Ausdrücke anführen können. Bekannt ist, dass directe Methoden oft ziemlich weitläufig ausfallen, doch haftet dieser Übelstand nicht allen directen Methoden in der Theorie der Zahlen an, und deshalb glaubten wir nicht umhin zu können, zu zeigen, wieviel sie hier zu leisten vermögen. Auch mag hier bemerkt werden, dass es nicht in unserer Absicht liegt, die besonderen Kunstgriffe, die sich dem Geübten nicht selten darbieten, ausführlicher zu entwickeln.

Zusammenhang zwischen den Indices in verschiedenen Systemen.

69.

Wir kehren jetzt zu den Wurzeln, die wir primitive genannt haben, zurück. Wir zeigen, dass, wenn eine beliebige primitive Wurzel zur Basis genommen wird, alle Zahlen, deren Indices prim zu $p-1$ sind, ebenfalls primitive Wurzeln sind, dass es aber ausser diesen keine weiter giebt, so dass dadurch zugleich unmittelbar die Anzahl der primitiven Wurzeln bekannt ist. (Man sehe Artikel 53.) Welche primitive Wurzel wir aber zur Basis nehmen wollen, ist im Allgemeinen unserem Belieben überlassen, woraus erhellt, dass es auch hier, wie bei der logarithmischen Rechnung, gewissermassen mehrere Systeme geben könne*); wir wollen zusehen, in welcher Weise sie mit einander verknüpft sind. Es seien a und b zwei primitive Wurzeln und m irgend eine andere Zahl, und es sei, wenn a zur Basis genommen wird, der Index von $b \equiv \beta$, der Index von m aber $\equiv \mu$ (mod. $p-1$); wenn aber b zur Basis genommen wird, so sei der Index von $a \equiv \alpha$, der Index von m aber $\equiv \nu$ (mod. $p-1$). Alsdann ist $\alpha\beta \equiv 1$ (mod. $p-1$). Denn es ist $a^\beta \equiv b$, daher $a^{\alpha\beta} \equiv b^\alpha \equiv a$ (mod. p) nach Voraussetzung, somit $\alpha\beta \equiv 1$ (mod. $p-1$). Durch analoge Schlüsse findet man $\nu \equiv \alpha\mu$ und $\mu \equiv \beta\nu$ (mod. $p-1$). Hat man daher eine Tafel der Indices, welche für die Basis a construiert ist, so lässt sich dieselbe leicht in eine andere verwandeln, deren Basis b ist. Denn wenn für die Basis a der Index von b congruent β ist, so ist für die Basis b der Index von a congruent $\frac{1}{\beta}$ (mod. $p-1$), und wenn man mit dieser Zahl alle Indices der Tafel multipliciert, so erhält man alle Indices für die Basis b.

---

*) Nur darin besteht ein Unterschied, dass bei den Logarithmen die Anzahl der Systeme unendlich gross, hier aber nur so gross ist, als die Anzahl der primitiven Wurzeln. Denn offenbar erzeugen congruente Grundzahlen dasselbe System.

70.

Obwohl aber eine gegebene Zahl mehrere Indices erhalten kann, wenn man andere und andere primitive Wurzeln zur Basis nimmt, so werden dieselben doch darin übereinstimmen, dass sie sämtlich mit $p - 1$ ein und denselben grössten gemeinschaftlichen Teiler haben. Denn wenn für die Basis a der Index einer gegebenen Zahl m, für die Basis b aber n ist und die grössten diesen Indices mit $p - 1$ gemeinschaftlichen Teiler μ, ν als ungleich vorausgesetzt werden, so wird der eine derselben der grössere, z. B. $\mu > \nu$, sein, und es wird daher μ in n nicht aufgehen. Bezeichnet man aber den Index von a, wenn b zur Basis genommen wird, mit α, so ist nach vorigem Artikel $n \equiv \alpha m$ (mod. $p - 1$) und daher wird μ auch in n aufgehen, was unserer Annahme widerspricht.

Dass dieser grösste, den Indices einer gegebenen Zahl und der Zahl $p - 1$ gemeinschaftliche Teiler von der Basis nicht abhängt, geht auch daraus hervor, dass er gleich $\frac{p-1}{t}$ ist, wo t den Exponenten bezeichnet, zu welchem die Zahl, von deren Indices die Rede ist, gehört. Denn wenn der Index für eine beliebige Basis gleich k ist, so ist t die kleinste Zahl (die Null ausgeschlossen) von der Art, dass das Product aus k und t ein Vielfaches von $p - 1$ wird (Vgl. Artikel 48 u. 58), oder es ist der kleinste Wert des Ausdrucks $\frac{0}{k}$ (mod. $p - 1$) ausser Null; dass dieser aber gleich dem grössten gemeinschaftlichen Teiler der Zahlen k und $p - 1$ ist, geht aus Artikel 29 ohne Schwierigkeit hervor.

71.

Man beweist ferner leicht, dass man die Basis stets so nehmen kann, dass die zum Exponenten t gehörige Zahl einen beliebig gegebenen Index, sofern dessen grösster mit $p - 1$ gemeinschaftlicher Teiler gleich $\frac{p-1}{t}$ ist, erhält. Bezeichnen wir diesen grössten gemeinschaftlichen Teiler der Kürze wegen mit d, ist ferner der gegebene Index $\equiv dm$ und der Index der gegebenen Zahl, wenn eine beliebige primitive Wurzel a zur Basis genommen wird, $\equiv dn$, so werden m und n zu $\frac{p-1}{d}$ oder t prim sein. Wenn dann ε der Wert des Ausdrucks $\frac{dm}{dn}$ (mod. $p - 1$) und zugleich prim zu $p - 1$ ist, so wird a^{ε} eine primitive Wurzel sein, und wenn diese zur Basis genommen wird, so wird, wie verlangt wurde, die gegebene Zahl den Index dm erhalten (denn es ist $a^{\varepsilon dm} \equiv a^{dn} \equiv$ der gegebenen Zahl). Dass aber der Ausdruck $\frac{dn}{dm}$ (mod. $p - 1$) zu $p - 1$ prime Werte besitzt, lässt sich folgendermassen beweisen. Jener Ausdruck ist nach Artikel 31,2 dem folgenden äquivalent:

$\frac{n}{m}\left(\text{mod. } \frac{p-1}{d}\right)$ oder $\frac{n}{m}$ (mod. t), und alle Werte desselben sind prim zu t; denn wenn irgend ein Wert e mit t einen gemeinschaftlichen Teiler hätte, so müsste dieser Teiler auch in me und daher auch in n, welcher Zahl me nach dem Modul t congruent ist, aufgehen. Dies ist aber gegen die Voraussetzung, nach welcher n prim zu t ist. Wenn also sämtliche Primteiler von $p-1$ auch in t aufgehen, so werden sämtliche Werte des Ausdrucks $\frac{n}{m}$ (mod. t) zu $p-1$ prim und die Anzahl derselben gleich d sein. Wenn aber $p-1$ noch andere Primteiler $f, g, h, \ldots$ hat, die in t nicht aufgehen, so werde irgend ein Wert des Ausdrucks $\frac{n}{m}$ (mod. t) $\equiv e$ gesetzt. Dann lässt sich aber, weil $t, f, g, h, \ldots$ sämtlich prim zu einander sind, eine Zahl ε finden, welche nach dem Modul t der Zahl e, nach den Moduln $f, g, h, \ldots$ aber beliebigen zu diesen respective primen Zahlen congruent wird (Artikel 32). Eine solche Zahl wird daher durch keinen Primfactor von $p-1$ teilbar und somit prim zu $p-1$ sein, wie verlangt. Schliesslich ergiebt sich aus der Theorie der Combinationen ohne Schwierigkeit, dass die Anzahl solcher Werte gleich $\frac{p-1}{t} \cdot \frac{f-1}{f} \cdot \frac{g-1}{g} \cdot \frac{h-1}{h} \cdots$ ist. Um aber diesen Exkurs nicht allzuweit auszudehnen, übergehen wir den Beweis, da er für unseren Zweck nicht so sehr erforderlich ist.

Besonderen Zwecken dienende Grundzahlen.

72.

Obwohl es im Allgemeinen völlig willkürlich ist, welche primitive Wurzel zur Basis genommen wird, können doch zuweilen die einen Grundzahlen besondere Vorteile vor andern gewähren. In Tafel I haben wir stets die Zahl 10, sobald sie primitive Wurzel war, zur Basis genommen; anderswo haben wir die Basis immer so bestimmt, dass der Index der Zahl 10 möglichst klein, d. i. $= \frac{p-1}{t}$ wurde, wo t den Exponenten bezeichnet, zu welchem 10 gehört. Welchen Vorteil wir hiervon haben, werden wir im sechsten Abschnitt zeigen, wo dieselbe Tafel noch zu andern Zwecken angewendet werden wird. Da aber auch hier noch etwas Willkürliches übrig bleiben kann, so haben wir, um etwas Bestimmtes festzusetzen, von allen primitiven Wurzeln, welche das Gesuchte leisten, immer die kleinste zur Basis gewählt. So hat z. B. für $p = 73$, wobei $t = 8$ und $d = 9$ ist, a^{ε} $\frac{72 \cdot 2}{8 \cdot 3} = 6$ Werte, nämlich die Werte 5, 14, 20, 28, 39, 40. Wir haben daher den kleinsten 5 zur Basis genommen.

Methode zur Bestimmung der primitiven Wurzeln.

73.

Die Methoden, die primitiven Wurzeln zu finden, beruhen zum grossen Teil auf Versuchen. Vergleicht man das, was wir im Artikel 55 vorgetragen haben, mit dem, was wir unten über die Lösung der Congruenz $x^n \equiv 1$ angeben werden, so hat man so ziemlich Alles, was sich durch directe Methoden leisten lässt. Euler gesteht in *Opusc. Analyt. T. I p. 152,* dass es äusserst schwierig zu sein scheine, solche Zahlen zu finden und dass ihr eigentliches Wesen zu den tiefsten Geheimnissen der Zahlen zu rechnen sei. Aber durch Probieren können sie ziemlich leicht in folgender Weise bestimmt werden. Der Geübte wird wissen, dass man die Weitläufigkeit des Verfahrens durch mannigfache besondere Kunstgriffe abkürzen kann; doch lernt man diese viel schneller durch praktische Übung als durch theoretische Vorschriften kennen.

1. Man nehme nach Belieben eine zu p (so werden wir stets den Modul bezeichnen) prime Zahl a (meistens ist es der Kürze der Rechnung wegen gut, sie möglichst klein, z. B. die Zahl 2, zu nehmen) und bestimme deren Periode (Artikel 46), d. i. die kleinsten Reste ihrer Potenzen, bis man zu einer Potenz a^t gelangt, deren kleinster Rest 1 ist.*) Ist nun $t = p - 1$, so ist a eine primitive Wurzel.

2. Ist aber $t < p - 1$, so nehme man eine andere Zahl b, welche in der Periode von a nicht enthalten ist, und suche in ähnlicher Weise deren Periode. Bezeichnet man den Exponenten, zu welchem b gehört, mit u, so erkennt man leicht, dass u weder gleich t noch ein aliquoter Teiler von t sein kann; denn in beiden Fällen würde $b^t \equiv 1$ werden, was nicht möglich ist, da die Periode von a alle Zahlen umfasst, deren t^{te} Potenz der Einheit congruent ist (Artikel 53). Wenn nun $u = p - 1$ wäre, so würde b eine primitive Wurzel sein; wenn aber u zwar nicht gleich $p - 1$, aber doch ein Vielfaches von t ist, so haben wir das gewonnen, dass wir eine zu einem grösseren Exponenten gehörige Zahl kennen und somit unsrem Ziele, welches in der Auffindung der zum grössten Exponenten gehörigen Zahl besteht, bereits näher sind. Wenn dagegen u weder gleich $p - 1$ noch ein Vielfaches von t ist, so können wir doch eine Zahl finden, welche zu einem Exponenten, der grösser als t und u ist, gehört, nämlich zu einem Exponenten gehört, der gleich dem kleinsten gemeinschaftlichen Dividuus der Zahlen t und u ist. Ist dieser Exponent gleich y, so löse man y derart in zwei zu einander prime Factoren m, n auf, dass der eine in t, der andere

*) Man wird von selbst einsehen, dass man nicht diese Potenzen selbst zu wissen braucht, da der kleinste Rest einer jeden leicht aus dem kleinsten Rest der vorhergehenden Potenz erhalten werden kann.

in u aufgeht.*) Ist dann ferner $a^{\frac{t}{m}} \equiv A$, $b^{\frac{u}{n}} \equiv B$ (mod. p), so wird das Product AB die zum Exponenten y gehörige Zahl sein. Denn es ist leicht ersichtlich, dass A zum Exponenten m, B zum Exponenten n gehört; daher wird das Product AB zu mn gehören, weil m und n prim zu einander sind, was auf ganz dieselbe Weise wie in Artikel 55 II bewiesen werden kann.

3. Wenn nun $y = p - 1$ ist, so wird AB eine primitive Wurzel sein. Ist dieses aber nicht der Fall, so muss man in analoger Weise wie vorher eine andere Zahl nehmen, welche in der Periode von AB nicht vorkommt. Diese wird entweder eine primitive Wurzel sein, oder sie wird zu einem Exponenten, der grösser als y ist, gehören oder es wird wenigstens vermittelst derselben (wie vorher) eine Zahl, die zu einem Exponenten, der grösser als y ist, gehört, gefunden werden können. Da somit die Zahlen, welche aus der Wiederholung dieser Operation hervorgehen, zu fortwährend wachsenden Exponenten gehören, so ist klar, dass schliesslich eine Zahl, die zu dem grössten Exponenten gehört, d. h. also eine primitive Wurzel ist, gefunden werden wird.

74.

Durch ein **Beispiel** werden diese Vorschriften deutlicher werden. Die Zahl, für welche die primitive Wurzel gesucht wird, sei $p = 73$. Man probiere zunächst die Zahl 2, deren Periode die folgende ist:

1.	2.	4.	8.	16.	32.	64.	55.	37.	1.	...
0.	1.	2.	3.	4.	5.	6.	7.	8.	9.	...

Da somit bereits die Potenz mit dem Exponenten 9 der Einheit congruent ist, so ist 2 keine primitive Wurzel. Man versuche also eine andere in der Periode von 2 nicht vorkommende Zahl, z. B. die Zahl 3, deren Periode ist:

1.	3.	9.	27.	8.	24.	72.	70.	64.	46.	65.	49.	1.	...
0.	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	...

Es ist daher auch 3 keine primitive Wurzel. Der kleinste gemeinschaftliche Dividuus der Exponenten, zu welchen 2 und 3 gehören (d. i. der Zahlen 9 und 12), ist 36 und dieser giebt nach den Vorschriften des vorigen Artikels zer-

*) Wie dies geschehen kann, ergiebt sich leicht aus Artikel 18. Man zerlege y in solche Factoren, die entweder selbst von einander verschiedene Primzahlen oder Potenzen verschiedener Primzahlen sind. Jeder von diesen geht in einer der beiden Zahlen t und u (oder auch in beiden) auf. Man schreibe sie einzeln entweder neben die Zahl t oder neben die Zahl u, je nachdem sie in jener oder dieser aufgehen. Geht einer in beiden auf, ist es gleichgültig, neben welche man ihn schreibt. Ist das Product der Factoren, welche neben t geschrieben sind, gleich m, das der übrigen gleich n, so sieht man leicht, dass m in t und n in u aufgeht und dass $mn = y$ ist.

legt die Factoren 9 und 4. Man erhebe nun 2 zur Potenz mit dem Exponenten 3. Das Product aus diesen, nämlich 54, wird somit zum Exponenten 36 gehören. Wenn man schliesslich die Periode von 54 berechnet und eine in dieser nicht enthaltene Zahl, z. B. die Zahl 5, von Neuem probiert, so wird man finden, dass diese eine primitive Wurzel ist.

Verschiedene Sätze über Perioden und primitive Wurzeln.

75.

Bevor wir diesen Gegenstand verlassen, wollen wir **einige Sätze** anführen, die ihrer Einfachheit wegen der Beachtung nicht unwert erscheinen.

Das Product aus allen Gliedern der Periode irgend einer Zahl ist $\equiv +1$, wenn ihre Anzahl oder der Exponent, zu welchem die Zahl gehört, ungerade ist, und $\equiv -1$, wenn jener Exponent gerade ist.

Beispiel. Für den Modul 13 besteht die Periode der Zahl 5 aus den Gliedern 1, 5, 12, 8, deren Product $480 \equiv -1 \pmod{13}$ ist.

Nach eben demselben Modul besteht die Periode der Zahl 3 aus den Gliedern 1, 3, 9, deren Product $27 \equiv 1 \pmod{13}$ ist.

Beweis. Ist der Exponent, zu welchem die Zahl gehört, t und der Index der Zahl selbst $\frac{p-1}{t}$, was nach Artikel 71 immer möglich ist, wenn die Basis richtig bestimmt wird, so ist der Index des Products aus allen Gliedern der Periode

$$\equiv (1+2+3+\cdots+t-1)\,\frac{p-1}{t} = \frac{(t-1)(p-1)}{2},$$

d. h. $\equiv 0 \pmod{p-1}$, wenn t ungerade, und $\equiv \frac{p-1}{2}$, wenn t gerade ist. Daher ist in ersterem Falle jenes Product $\equiv 1 \pmod{p}$, in letzterem aber $\equiv -1 \pmod{p}$ (Artikel 62).

76.

Wenn in dem vorigen Satze die Zahl eine primitive Wurzel ist, so umfasst die Periode derselben alle Zahlen $1, 2, 3, \ldots, p-1$, deren Product somit stets $\equiv -1$ ist (denn $p-1$ ist stets gerade, den einen Fall $p=2$ ausgenommen, in welchem -1 und $+1$ äquivalent sind).

Dieser elegante Satz, der gewöhnlich folgendermassen ausgesprochen wird: Das um die Einheit vermehrte Product aller Zahlen, die kleiner als eine gegebene Primzahl sind, ist durch diese Primzahl teilbar, wurde zuerst von Waring veröffentlicht und von diesem Wilson zugeschrieben *(Meditationes algebraicae, ed. 3. pag. 380).* Aber keiner von beiden konnte ihn beweisen, und Waring gesteht, dass der Beweis um so schwieriger erscheine, weil man sich keine Bezeichnung denken

könne, welche eine Primzahl auszudrücken vermöchte. — Nach unserer Meinung aber müssen derartige Wahrheiten vielmehr aus Begriffen denn aus Bezeichnungen geschöpft werden. Später hat Lagrange einen Beweis gegeben *(Nouv. Mém. de l'Académie de Berlin, 1771).* Derselbe stützt sich auf die Betrachtung der Coefficienten, welche sich aus der Entwicklung des Productes

$$(x+1)(x+2)(x+3)\ldots.(x+p-1)$$

ergeben. Setzt man nämlich dieses Product

$$= x^{p-1} + Ax^{p-2} + Bx^{p-3} + \cdots + Mx + N,$$

so werden die Coefficienten $A, B, \ldots, M$ durch p teilbar sein, während $N = 1 \cdot 2 \cdot 3 \cdots (p-1)$ ist. Nun ist für $x = 1$ das Product durch p teilbar; alsdann aber wird dasselbe $\equiv 1 + N$ (mod. p), somit lässt sich notwendig $1 + N$ durch p teilen.

Schliesslich hat Euler in *Opusc. analyt. T. 1. p. 329* einen Beweis gegeben, der mit dem unsrigen übereinstimmt. Da nun solche Männer diesen Satz ihres Nachdenkens über ihn nicht unwert erachtet haben, hoffen wir keinem Tadel zu begegnen, wenn wir noch einen Beweis hierhersetzen.

77.

Wenn das Product zweier Zahlen a und b nach dem Modul p der Einheit congruent ist, wollen wir diese Zahlen a und b nach Euler einander **associiert** nennen. Dann wird nach dem vorhergehenden Abschnitte jede positive Zahl, die kleiner als p ist, eine und nur eine associierte positive Zahl haben, die ebenfalls kleiner als p ist. Nun kann man aber leicht beweisen, dass von den Zahlen $1, 2, 3, \ldots, p-1$ nur allein 1 und $p-1$ sich selbst associiert sind. Denn da die sich selbst associierten Zahlen Wurzeln der Congruenz $x^2 \equiv 1$ sind und diese vom zweiten Grade ist, so kann dieselbe nicht mehr als zwei d. h. keine andern Wurzeln als 1 und $p-1$ haben. Lässt man daher diese bei Seite, so werden von den übrigen Zahlen $2, 3, \ldots, p-2$ je zwei associiert, also ihr Product $\equiv 1$ sein. Somit ist auch das Product aus allen, nämlich $1 \cdot 2 \cdot 3 \cdots (p-1) \equiv p-1$ oder $\equiv -1$.

Z. B. sind nach dem Modul 13 von den Zahlen $2, 3, 4, \ldots, 11$ die folgenden zu einander associiert: 2 und 7, 3 und 9, 4 und 10, 5 und 8, 6 und 11; denn es ist $2 \cdot 7 \equiv 1$, $3 \cdot 9 \equiv 1$, u. s. w. Daher ist $2 \cdot 3 \cdot 4 \cdots 11 \equiv 1$ und somit $1 \cdot 2 \cdot 3 \cdots 12 \equiv -1$.

78.

Man kann aber auch den Wilson'schen Satz allgemeiner so aussprechen. Das Product aus allen Zahlen, welche kleiner als irgend eine gegebene Zahl A und zugleich prim zu ihr sind, ist nach dem Modul A der entweder negativ oder positiv ge-

nommenen Einheit congruent. Die Einheit ist negativ zu nehmen, wenn A von der Form p^m oder $2p^m$ ist, wo p eine von 2 verschiedene Primzahl bezeichnet, und überdies, wenn $A = 4$ ist, positiv aber in allen übrigen Fällen. Der Satz, wie er von Wilson angegeben wurde, ist unter dem ersten Falle enthalten. — Z. B. ist für $A = 15$ das Product aus den Zahlen 1, 2, 4, 7, 8, 11, 13, $14 \equiv 1$ (mod. 15). Einen Beweis fügen wir der Kürze wegen nicht hinzu; nur bemerken wir, dass derselbe auf ähnliche Weise geführt werden kann wie im vorigen Artikel, nur dass die Congruenz $x^2 \equiv 1$ mehr als zwei Wurzeln haben kann, welche gewisse besondere Betrachtungen erfordern. Es könnte auch der Beweis aus der Betrachtung der Indices ähnlich wie in Artikel 75 abgeleitet werden, wenn man das, was wir sogleich über die zusammengesetzten Moduln sagen werden, hinzunimmt.

79.

Wir kehren nun zur Aufzählung der anderen Sätze zurück (Artikel 75).

Die Summe aller Glieder der Periode einer beliebigen Zahl ist $\equiv 0$. So ist im Beispiel des Artikel 75: $1 + 5 + 12 + 8 = 26 \equiv 0$ (mod. 13).

Beweis. Ist die Zahl, um deren Periode es sich handelt, gleich a, und der Exponent, zu welchem sie gehört, gleich t, so ist die Summe aller Glieder der Periode:

$$\equiv 1 + a + a^2 + a^3 + \cdots + a^{t-1} \equiv \frac{a^t - 1}{a - 1} \pmod{p}.$$

Nun ist aber $a^t - 1 \equiv 0$; daher ist diese Summe immer $\equiv 0$ (Artikel 22), wofern nicht etwa $a - 1$ durch p teilbar oder $a \equiv 1$ ist. Diesen Fall müssen wir also ausnehmen, wenn wir auch ein einziges Glied eine Periode nennen wollen.

80.

Das Product aller primitiven Wurzeln ist $\equiv 1$, den einen Fall $p = 3$ ausgenommen, denn in diesem giebt es nur die eine primitive Wurzel 2.

Beweis. Wird eine beliebige primitive Wurzel zur Basis genommen, so werden die Indices aller primitiven Wurzeln Zahlen sein, die prim zu $p - 1$ und zugleich kleiner als $p - 1$ sind. Aber die Summe dieser Zahlen d. h. der Index des Products aus allen primitiven Wurzeln ist $\equiv 0$ (mod. $p - 1$) und daher das Product selbst $\equiv 1$ (mod. p); denn man sieht leicht, dass, wenn k eine zu $p - 1$ prime Zahl ist, auch $p - 1 - k$ zu $p - 1$ prim sein wird und dass somit je zwei solche zu $p - 1$ prime Zahlen eine Summe bilden, die durch $p - 1$ teilbar ist; (k kann nämlich nie gleich $p - 1 - k$ sein, ausser in dem Falle $p - 1 = 2$ oder $p = 3$, den wir ausgenommen haben; denn offenbar ist in allen übrigen Fällen $\frac{p-1}{2}$ nicht prim zu $p - 1$).

81.

Die Summe aller primitiven Wurzeln ist entweder $\equiv 0$ (wenn $p-1$ durch irgend ein Quadrat teilbar ist) oder $\equiv \pm 1 \pmod{p}$ (wenn $p-1$ das Product ungleicher Primzahlen ist; hierbei ist das positive oder negative Zeichen zu nehmen, je nachdem die Anzahl dieser Primzahlen gerade oder ungerade ist).

Beispiel. 1) Für $p=13$ hat man die primitiven Wurzeln 2, 6, 7, 11, deren Summe $26 \equiv 0 \pmod{p}$ ist. — 2) Für $p=11$ sind die primitiven Wurzeln 2, 6, 7, 8, deren Summe $23 \equiv +1 \pmod{11}$ ist. — 3) Für $p=31$ sind die primitiven Wurzeln 3, 11, 12, 13, 17, 21, 22, 24, deren Summe $123 \equiv -1 \pmod{31}$ ist.

Beweis. Wir haben oben (Artikel 55, II) bewiesen, dass, wenn $p-1 = a^\alpha b^\beta c^\gamma \ldots$ (wo $a, b, c, \ldots$ ungleiche Primzahlen sind) ist und $A, B, C, \ldots$ irgend welche respective zu den Exponenten $a^\alpha, b^\beta, c^\gamma, \ldots$ gehörende Zahlen sind, alsdann sämtliche Producte $ABC\ldots$ primitive Wurzeln darstellen. Man kann aber auch leicht beweisen, dass jede primitive Wurzel durch ein solches Product dargestellt werden kann und zwar nur auf eine einzige Weise.*)

Hieraus folgt, dass man diese Producte an Stelle der primitiven Wurzeln nehmen kann. Da aber in diesen Producten alle Werte von A mit allen Werten von B u. s. w. combiniert werden müssen, so ist die Summe aller dieser Producte gleich dem Product aus der Summe aller Werte von A in die Summe aller Werte von B in die Summe aller Werte von C u. s. w., wie in der Theorie der Combinationen gezeigt wird. Bezeichnet man alle Werte von $A, B, \ldots$ bezüglich durch $A, A', A'', \ldots$; $B, B', B'', \ldots\ldots$, so wird die Summe aller primitiven Wurzeln

$$\equiv (A + A' + A'' + \cdots)(B + B' + B'' + \cdots)\cdots$$

Ich behaupte nun, dass, wenn der Exponent $\alpha = 1$ ist, die Summe $A + A' + A'' + \cdots \equiv -1 \pmod{p}$ wenn aber $\alpha > 1$ ist, diese Summe $\equiv 0$ sein wird und analog bei den andern $\beta, \gamma, \ldots$. Sobald dieses bewiesen ist, erhellt die Richtigkeit unseres Satzes ohne Weiteres. Denn wenn $p-1$ durch eine Quadratzahl teilbar ist, so wird irgend einer der Exponenten $\alpha, \beta, \gamma, \ldots$ die Einheit übersteigen und daher wird irgend einer der Factoren, deren Producte die Summe aller primitiven Wurzeln congruent ist, $\equiv 0$ und somit auch das Product selbst $\equiv 0$ sein. Wenn aber $p-1$ durch keine Quadrat-

*) Man bestimme nämlich Zahlen $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$ so, dass $\mathfrak{a} \equiv 1 \pmod{a^\alpha}$ und $\equiv 0 \pmod{b^\beta c^\gamma \ldots}$, $\mathfrak{b} \equiv 1 \pmod{b^\beta}$ und $\equiv 0 \pmod{a^\alpha c^\gamma \ldots}$ u. s. w. wird (vgl. Artikel 32). Dann ist $\mathfrak{a} + \mathfrak{b} + \mathfrak{c} + \cdots \equiv 1 \pmod{p-1}$ (Artikel 19). Wenn nun irgend eine primitive Wurzel r durch ein Product $ABC\ldots$ dargestellt werden soll, so nehme man $A \equiv r^\mathfrak{a}$, $B \equiv r^\mathfrak{b}$, $C \equiv r^\mathfrak{c}, \ldots$; dann wird A zum Exponenten a^α, B zum Exponenten b^β, u. s. w. gehören und es wird das Product aus allen $A, B, C, \ldots \equiv r \pmod{p}$ sein. Schliesslich sieht man leicht, dass $A, B, C, \ldots$ auf keine andere Weise bestimmt werden können.

zahl teilbar ist, so werden sämtliche Exponenten $\alpha, \beta, \gamma, \ldots$ gleich 1 sein; demnach wird die Summe aller primitiven Wurzeln dem Producte aus soviel Factoren, von denen jeder $\equiv -1$ ist, congruent, als es Zahlen $a, b, c, \ldots$ giebt, und daher $\equiv \pm 1$, je nachdem die Anzahl dieser Zahlen gerade oder ungerade ist. Jene Behauptungen werden aber folgendermassen bewiesen.

1) Wenn $\alpha = 1$ und A die zum Exponenten a gehörige Zahl ist, so sind die andern zu diesem Exponenten gehörigen Zahlen $A^2, A^3, \ldots, A^{a-1}$. Nun ist aber

$$1 + A + A^2 + A^3 + \cdots + A^{a-1}$$

die Summe der vollständigen Periode und daher $\equiv 0$ (Artikel 79); somit:

$$A + A^2 + A^3 + \cdots + A^{a-1} \equiv -1.$$

2) Ist aber $\alpha > 1$ und A die zum Exponenten a^α gehörige Zahl, so erhält man die anderen zu diesem Exponenten gehörigen Zahlen, wenn man von den Zahlen $A^2, A^3, A^4, \ldots, A^{a^\alpha - 1}$ die Zahlen $A^a, A^{2a}, A^{3a}, \ldots$ weglässt (vgl. Artikel 53). Daher ist die Summe derselben

$$\equiv 1 + A + A^2 + \cdots + A^{a^\alpha - 1} - (1 + A^a + A^{2a} + \cdots + A^{a^\alpha - a})$$

d. h. congruent der Differenz zweier Perioden und somit $\equiv 0$.

Über Moduln, welche Potenzen von Primzahlen sind.

82.

Alles, was wir bisher auseinandergesetzt haben, stützt sich auf die Annahme, dass der Modul eine Primzahl ist. Es bleibt noch der Fall zu betrachten, wo für den Modul eine **zusammengesetzte** Zahl genommen wird. Da jedoch hier weder so elegante Eigenschaften zum Vorschein kommen, wie im ersteren Falle, noch auch besonders feine Kunstgriffe nötig sind, um sie zu finden, vielmehr beinahe alles aus der blossen Anwendung der vorher dargelegten Prinzipien abgeleitet werden kann, so würde es überflüssig und ermüdend sein, hier alle Einzelheiten zu erschöpfen. Wir wollen daher nur kurz auseinandersetzen, was diesem Fall mit dem vorigen gemeinsam und was ihm eigentümlich ist.

83.

Die Sätze der Artikel 45—48 sind bereits allgemein bewiesen; der Satz des Artikel 49 muss aber folgendermassen abgeändert werden.

Bezeichnet f die Anzahl der Zahlen, die prim zu m und zugleich kleiner als m sind, d. h. ist $f = \varphi(m)$ (Artikel 38), so ist der Exponent t der niedrigsten Potenz einer gegebenen zu m primen Zahl a, welche nach dem Modul m der Einheit congruent ist, entweder gleich f oder ein aliquoter Teil dieser Zahl.

Der Beweis des Satzes im Artikel 49 kann auch für diesen Fall gelten, wenn man nur m an die Stelle von p, f an Stelle von $p-1$ und an Stelle der Zahlen $1, 2, 3, \ldots, p-1$ die Zahlen setzt, welche prim zu m und zugleich kleiner als m sind. Wir weisen daher den Leser hierauf hin. Übrigens lassen sich die übrigen Beweise, von denen wir dort (Artikel 50, 51) gesprochen haben, nicht ohne grosse Weitläufigkeiten auf diesen Fall anwenden. Hinsichtlich der folgenden Sätze aber (Artikel 52 u. ff.) herrscht ein grosser Unterschied zwischen den Moduln, welche Potenzen von Primzahlen sind, und denen, welche durch mehrere Primzahlen sich teilen lassen. Wir werden daher die Moduln der ersten Art für sich betrachten.

84.

Ist der Modul $m = p^n$, wo p eine Primzahl bezeichnet, so wird $f = p^{n-1}(p-1)$ (Artikel 38). Wenn man nun die Untersuchungen in den Artikeln 53, 54 auf diesen Fall anwendet, so wird man, wenn man die im vorigen Artikel angegebenen Änderungen vornimmt, finden, das alles dort Bewiesene auch für diesen Fall gültig ist, wofern nur vorher der Beweis geführt ist, dass die Congruenz von der Form $x^t - 1 \equiv 0 \pmod{p^n}$ nicht mehr als t verschiedene Wurzeln haben kann. Für einen Primzahlmodul haben wir diese Thatsache aus dem allgemeinen Satze des Artikel 43 abgeleitet, der jedoch in seiner ganzen Ausdehnung nur von Primzahlmoduln gilt und daher nicht auf diesen Fall angewendet werden darf. Wir werden indessen mittelst einer besonderen Methode beweisen, dass der Satz auch für diesen besonderen Fall richtig ist. Weiter unten (Abschnitt VIII) werden wir dasselbe leichter finden lehren.

85.

Wir wollen folgenden **Satz** beweisen:

Ist e der grösste gemeinschaftliche Teiler der Zahlen t und $p^{n-1}(p-1)$, so besitzt die Congruenz $x^t \equiv 1 \pmod{p^n}$ e verschiedene Wurzeln.

Es sei $e = kp^\nu$, so dass k den Factor p nicht enthält und daher in der Zahl $p-1$ aufgeht. Dann wird die Congruenz $x^t \equiv 1$ nach dem Modul p k verschiedene Wurzeln haben, und wenn man diese durch $A, B, C, \ldots$ bezeichnet, so wird jede Wurzel derselben Congruenz nach dem Modul p^n irgend einer der Zahlen $A, B, C, \ldots$ nach dem Modul p congruent sein müssen. Wir werden nun beweisen, dass die Congruenz $x^t \equiv 1 \pmod{p^n}$ p^ν Wurzeln hat, die A, ebenso viele, die B, u. s. w. nach dem Modul p congruent sind. Daraus folgt dann, dass die Anzahl aller Wurzeln gleich kp^ν oder gleich e ist, wie behauptet wurde. Jenen Beweis aber werden wir in der Weise führen, dass wir zuerst zeigen, dass, wenn α eine zu A nach dem Modul p congruente Wurzel ist, auch

$$\alpha + p^{n-\nu},\ \alpha + 2p^{n-\nu},\ \alpha + 3p^{n-\nu},\ \ldots,\ \alpha + (p^\nu - 1)p^{n-\nu}$$

Wurzeln sind; zweitens, dass andere mit A nach dem Modul p congruente Zahlen als die, welche in der Form $\alpha + hp^{n-\nu}$ (wo h eine beliebige ganze Zahl bezeichnet) enthalten sind, keine Wurzeln sein können, woraus folgt, dass man p^{ν} und nicht mehr verschiedene Wurzeln erhält. Dasselbe gilt von den Wurzeln, welche den einzelnen Zahlen $B, C, \ldots$ congruent sind. Drittens werden wir zeigen, wie man immer eine Wurzel, welche A nach dem Modul p congruent ist, finden kann.

86.

Satz: Wenn t wie im vorigen Artikel eine Zahl ist, die durch p^{ν} aber nicht durch $p^{\nu+1}$ teilbar ist, so wird

$$(\alpha + hp^{\mu})^t - \alpha^t \equiv 0 \pmod{p^{\mu+\nu}}, \text{ aber } \equiv \alpha^{t-1}hp^{\mu}t \pmod{p^{\mu+\nu+1}}.$$

Der letzte Teil des Satzes findet nicht statt, wenn $p = 2$ und zugleich $\mu = 1$ ist.

Der Beweis dieses Satzes könnte aus der Entwicklung der Potenz eines Binoms abgeleitet werden, wenn man zeigte, dass alle Glieder nach dem zweiten durch $p^{\mu+\nu+1}$ teilbar sind. Da jedoch die Betrachtung der Nenner der Coefficienten zu einigen Weitläufigkeiten führt, ziehen wir die folgende Methode vor.

Setzen wir zunächst $\mu > 1$ und $\nu = 1$ voraus, so wird, weil

$$x^t - y^t = (x-y)\,(x^{t-1} + x^{t-2}y + x^{t-3}y^2 + \cdots + y^{t-1})$$

ist,

$$(\alpha + hp^{\mu})^t - \alpha^t = hp^{\mu}[(\alpha + hp^{\mu})^{t-1} + (\alpha + hp^{\mu})^{t-2}\alpha + \cdots + \alpha^{t-1}].$$

Nun ist aber:

$$\alpha + hp^{\mu} \equiv \alpha \pmod{p^2}.$$

Daher wird jedes Glied $(\alpha + hp^{\mu})^{t-1}$, $(\alpha + hp^{\mu})^{t-2}\alpha, \ldots \equiv \alpha^{t-1} \pmod{p^2}$ und daher die Summe aller $\equiv t\alpha^{t-1} \pmod{p^2}$ oder von der Form $t\alpha^{t-1} + Vp^2$, wo V eine beliebige Zahl bezeichnet. Demnach wird $(\alpha + hp^{\mu})^t - \alpha^t$ von der Form:

$$\alpha^{t-1}hp^{\mu}t + Vhp^{\mu+2}, \quad \text{d. h. } \equiv \alpha^{t-1}hp^{\mu}t \pmod{p^{\mu+2}} \text{ und } \equiv 0 \pmod{p^{\mu+1}}$$

Für diesen Fall ist somit der Satz bewiesen.

Wenn nun der Satz, während immer noch $\mu > 1$ bleibt, für andere Werte von ν nicht richtig wäre, so würde es notwendig irgend eine Grenze geben, bis zu welcher der Satz stets richtig, über die hinaus er aber nicht richtig sein würde. Es sei der kleinste Wert von ν, für welchen er nicht mehr gilt, gleich φ. Dann sieht man leicht, dass, wenn t durch $p^{\varphi-1}$, nicht aber durch p^{φ} teilbar ist, der Satz noch richtig ist, dass er es jedoch nicht mehr ist, wenn man tp an die Stelle von t setzt. Wir haben daher:

$$(\alpha + hp^{\mu})^t \equiv \alpha^t + \alpha^{t-1}hp^{\mu}t \pmod{p^{\mu+\varphi}} \text{ oder } = \alpha^t + \alpha^{t-1}hp^{\mu}t + up^{\mu+\varphi},$$

wo u eine ganze Zahl bezeichnet. Da aber der Satz für $\nu = 1$ bereits bewiesen ist, so wird:

$$(\alpha^t + \alpha^{t-1}hp^\mu t + up^{\mu+\varphi})^p \equiv \alpha^{tp} + \alpha^{tp-1}hp^{\mu+1}t + \alpha^{tp-t}up^{\mu+\varphi+1} \pmod{p^{\mu+\varphi+1}}$$

und daher auch

$$(\alpha + hp^\mu)^{tp} \equiv \alpha^{tp} + \alpha^{tp-1}hp^\mu tp \pmod{p^{\mu+\varphi+1}},$$

d. h. der Satz ist auch richtig, wenn man tp für t setzt, d. i. auch für $\nu = \varphi$, was im Widerspruch steht mit unsrer Annahme. Daraus erhellt, dass der Satz für alle Werte von ν richtig ist.

87.

Es bleibt nur noch der Fall übrig, wo $\mu = 1$ ist. Mittelst einer Methode, die der im vorigen Artikel angewandten ganz ähnlich ist, kann man ohne Zuhülfenahme des Binomialtheorems beweisen, dass

$$(\alpha + hp)^{t-1} \equiv \alpha^{t-1} + \alpha^{t-2}(t-1)hp \pmod{p^2}$$
$$\alpha(\alpha + hp)^{t-2} \equiv \alpha^{t-1} + \alpha^{t-2}(t-2)hp$$
$$\alpha^2(\alpha + hp)^{t-3} \equiv \alpha^{t-1} + \alpha^{t-2}(t-3)hp$$
$$\cdots\cdots\cdots\cdots\cdots$$

ist, so dass das Aggregat (da die Anzahl der Teile gleich t ist) wird:

$$\equiv t\alpha^{t-1} + \frac{(t-1)t}{2}\alpha^{t-2}hp \pmod{p^2}.$$

Da aber t durch p teilbar ist, so wird auch $\frac{(t-1)t}{2}$ in allen Fällen durch p teilbar sein, ausgenommen den Fall, wo $p = 2$ ist, den wir schon im vorigen Artikel ausgeschlossen haben. In den übrigen Fällen aber wird $\frac{(t-1)t}{2}\alpha^{t-2}hp \equiv 0 \pmod{p^2}$ und daher auch jenes Aggregat $\equiv t\alpha^{t-1} \pmod{p^2}$, wie im vorigen Artikel. Im Übrigen ist der Beweis hier ebenso wie dort.

Wir schliessen daher allgemein, den einen Fall $p = 2$ ausgenommen, dass man hat:

$$(\alpha + hp^\mu)^t \equiv \alpha^t \pmod{p^{\mu+\nu}}$$

und $(\alpha + hp^\mu)^t$ nicht $\equiv \alpha^t$ für jeden Modul, der eine höhere Potenz von p ist als $p^{\mu+\nu}$, vorausgesetzt jedoch, dass h durch p nicht teilbar und p^ν die höchste Potenz von p ist, welche in der Zahl t aufgeht.

Hieraus leitet man sogleich die Sätze 1 und 2 ab, die wir uns im Artikel 85 zu beweisen vorgenommen hatten. Nämlich

erstens, wenn $\alpha^t \equiv 1$, so ist auch $(\alpha + hp^{n-\nu})^t \equiv 1 \pmod{p^n}$,

zweitens, wenn irgend eine Zahl α', welche A und daher auch α nach dem Modul p, der letzteren aber nicht nach dem Modul $p^{n-\nu}$ congruent ist, der Congruenz $x^t \equiv 1 \pmod{p^n}$ genügte, und wenn wir annehmen, dass $\alpha' = \alpha + lp^\lambda$ ist, so dass l durch p nicht teilbar ist, so wird $\lambda < n - \nu$; als-

dann aber ist $(\alpha + lp^{\lambda})^t \equiv \alpha^t$ nach dem Modul $p^{\lambda+\nu}$, aber nicht nach dem Modul p^n, welcher eine höhere Potenz von p ist. Demnach kann α' keine Wurzel der Congruenz $x^t \equiv 1$ sein.

88.

Drittens sollten wir irgend eine Wurzel der Congruenz $x^t \equiv 1 \pmod{p^n}$ finden, die A congruent ist. Wir werden hier nur zeigen, wie dies geschehen kann, wenn bereits eine Wurzel derselben Congruenz nach dem Modul p^{n-1} bekannt ist. Offenbar genügt dies, da wir vom Modul p, für welchen A eine Wurzel ist, zum Modul p^2 und so fort zu allen folgenden Potenzen übergehen können.

Es sei also α eine Wurzel der Congruenz $x^t \equiv 1 \pmod{p^{n-1}}$, und es werde gesucht die Wurzel derselben Congruenz nach dem Modul p^n, so setze man diese gleich $\alpha + hp^{n-\nu-1}$, welche Form dieselbe nach dem vorigen Artikel haben muss (den Fall, wo $\nu = n - 1$, werden wir nachher für sich betrachten; grösser aber als $n - 1$ kann ν nicht sein). Es muss also sein:

$$(\alpha + hp^{n-\nu-1})^t \equiv 1 \pmod{p^{n-1}}.$$

Nun ist aber:

$$(\alpha + hp^{n-\nu-1})^t \equiv \alpha^t + \alpha^{t-1}htp^{n-\nu-1} \pmod{p^n}.$$

Bestimmt man daher h so, dass $1 \equiv \alpha^t + \alpha^{t-1}htp^{n-\nu-1} \pmod{p^n}$ oder (weil nach Voraussetzung $1 \equiv \alpha^t \pmod{p^{n-1}}$ und t durch p^ν teilbar ist) so, dass $\frac{\alpha^t - 1}{p^{n-1}} + \alpha^{t-1}h\frac{t}{p^\nu}$ teilbar wird durch p, so hat man das Gesuchte gefunden. Dass dies aber immer möglich ist, geht aus dem vorhergehenden Abschnitt hervor, da wir angenommen haben, dass t durch keine höhere Potenz von p teilbar sein solle als durch p^ν und daher $a^{t-1}\frac{t}{p^\nu}$ zu p prim ist.

Ist aber $\nu = n - 1$ d. h. ist t durch p^{n-1} oder auch durch eine höhere Potenz von p teilbar, so wird jeder Wert A, welcher der Congruenz $x^t \equiv 1$ nach dem Modul p genügt, derselben auch nach dem Modul p^n genügen. Denn ist $t = p^{n-1}\tau$, so wird $t \equiv \tau \pmod{p-1}$; mithin wird, da $A^t \equiv 1 \pmod{p}$ ist, auch $A^\tau \equiv 1 \pmod{p}$. Setzt man also $A^\tau = 1 + hp$, so ist $A^t = (1 + hp)^{p^{n-1}} \equiv 1 \pmod{p^n}$ (Artikel 87).

89.

Alles, was wir im Artikel 57 u. ff. mit Hülfe des Satzes, dass die Congruenz $x^t \equiv 1$ nicht mehr als t verschiedene Wurzeln haben kann, abgeleitet haben, gilt auch für einen Modul, welcher eine Potenz einer Primzahl ist; und wenn wir **primitive Wurzeln** diejenigen Zahlen nennen, welche zum Exponenten $p^{n-1}(p-1)$ gehören oder in deren Perioden sich alle durch p nicht teilbaren Zahlen vorfinden, so wird es auch hier primitive Wurzeln geben. Alles ferner, was wir oben von den Indices und deren Anwendung,

sowie über die Auflösung der Congruenz $x^t \equiv 1$ angegeben haben, lässt sich auch auf diesen Fall anwenden. Da dies keinen Schwierigkeiten unterliegt, würde es überflüssig sein, alles vollständig zu wiederholen. Überdies haben wir gezeigt, wie man die Wurzeln der Congruenz $x^t \equiv 1$ nach dem Modul p^n aus den Wurzeln derselben Congruenz nach dem Modul p ableiten kann. Doch müssen wir noch Einiges über den Fall, wo irgend eine Potenz von 2 der Modul ist, einen Fall, den wir oben ausgenommen haben, hinzufügen.

Moduln, welche Potenzen von 2 sind.

90.

Wenn man irgend eine Potenz der Zahl 2, welcher höher ist als die zweite, z. B. 2^n zum Modul nimmt, so ist die Potenz mit dem Exponenten 2^{n-2} von jeder ungeraden Zahl der Einheit congruent.

Z. B. ist $3^8 = 6581 \equiv 1$ (mod. 32).

Denn jede ungerade Zahl ist entweder in der Form $1 + 4h$ oder in der Form $-1 + 4h$ enthalten, woraus der Satz unmittelbar folgt (Satz des Artikel 86).

Da somit der Exponent, zu welchem eine beliebige ungerade Zahl, nach dem Modul 2^n gehört, ein Teiler von 2^{n-2} sein muss, so wird jede Zahl zu einer von den folgenden Zahlen: $1, 2, 4, 8, \ldots, 2^{n-2}$ gehören. Zu welcher von diesen sie gehört, kann man leicht folgendermassen entscheiden. Ist die gegebene Zahl gleich $4h \pm 1$ und der Exponent der grössten Potenz von 2, welche in h aufgeht, gleich m (wo m auch gleich 0 sein kann, wenn nämlich h ungerade ist), so ist der Exponent, zu welchem die gegebene Zahl gehört, gleich 2^{n-m-2}, falls $n > m + 2$. Ist aber n gleich oder kleiner als $m + 2$, so ist die gegebene Zahl $\equiv \pm 1$ und gehört daher zum Exponenten 1 oder zum Exponenten 2. Denn wie aus Artikel 86 ohne Schwierigkeit hervorgeht, wird jede Zahl von der Form $\pm 1 + 2^{m+2}k$ (die der Form $4h \pm 1$ äquivalent ist), wenn man sie zu einer Potenz mit dem Exponenten 2^{n-m-2} erhebt, nach dem Modul 2^n der Einheit congruent; erhebt man sie aber zu einer Potenz mit einem Exponenten, der eine niedrigere Potenz von 2 ist, so ist sie der Einheit nicht congruent. Daher gehört jede Zahl von der Form $8k + 3$ oder $8k + 5$ zum Exponenten 2^{n-2}.

91.

Hieraus geht hervor, dass es hier primitive Wurzeln in dem Sinne, wie wir oben den Ausdruck aufgefasst haben, nicht giebt, nämlich keine Zahlen giebt, deren Periode alle Zahlen umfasst, die kleiner als der Modul und prim zu demselben sind. Trotzdem sieht man leicht, dass man auch hier etwas Analoges hat. Man findet nämlich, dass eine Potenz einer Zahl von der Form $8k + 3$ mit ungeraden Exponenten immer von der Form $8k + 3$,

eine Potenz aber mit geradem Exponenten immer von der Form $8k+1$ ist; keine Potenz kann also von der Form $8k+5$ oder $8k+7$ sein. Da somit die Periode einer Zahl von der Form $8k+3$ aus 2^{n-2} verschiedenen Gliedern besteht, deren jedes entweder von der Form $8k+3$ oder von der Form $8k+1$ ist, und es nicht mehr solcher Zahlen, welche kleiner als der Modul sind, giebt als 2^{n-2}, so ist offenbar jede Zahl von der Form $8k+1$ oder $8k+3$ nach dem Modul 2^n irgend einer Potenz einer beliebigen Zahl von der Form $8k+3$ congruent. Auf analoge Weise kann man zeigen, dass die Periode einer Zahl von der Form $8k+5$ alle Zahlen von den Formen $8k+1$ und $8k+5$ enthält. Wenn daher eine Zahl von der Form $8k+5$ zur Basis genommen wird, so werden alle Zahlen von der Form $8k+1$ und $8k+5$, positiv genommen, und alle Zahlen von der Form $8k+3$ und $8k+7$, negativ genommen, reelle Indices erhalten und zwar sind hier nach dem Modul 2^{n-2} congruente Indices als äquivalent zu betrachten. In dieser Weise ist unsere Tafel I zu verstehen, in welcher wir für die Moduln 16, 32 und 64 (denn für den Modul 8 ist keine Tafel nötig) stets die Zahl 5 zur Basis genommen haben. Z. B. entspricht der Zahl 19, welche von der Form $8n+3$ und daher negativ zu nehmen ist, für den Modul 64 der Index 7, was bedeutet, dass $5^7 \equiv -19$ (mod. 64) ist. Den negativ genommenen Zahlen von der Form $8n+1$ und $8n+5$ und den positiv genommenen Zahlen von der Form $8n+3$ und $8n+7$ aber würden gewissermassen imaginäre Indices beizulegen sein. Führte man diese ein, so könnte man die Rechnung mit den Indices auf einen sehr einfachen Algorithmus zurückführen. Da wir aber zu weit geführt werden würden, wollten wir dies in aller Strenge auseinandersetzen, so sparen wir uns diesen Punkt für eine andere Gelegenheit auf, wenn wir etwa die Theorie der imaginären Grössen, die nach unsrer Ansicht bisher von Niemand auf klare Begriffe zurückgeführt worden ist, darzulegen versuchen werden. Kundige werden diesen Algorithmus leicht selbst finden; minder Geübte werden trotzdem diese Tafel gebrauchen können, ebenso wie diejenigen, welche mit den neueren Untersuchungen über die imaginären Logarithmen nicht bekannt sind, sich der Logarithmen bedienen, wenn sie nur die oben dargelegten Prinzipien verstanden haben.

Aus mehreren Primzahlen zusammengesetzte Moduln.

92.

Hinsichtlich eines aus mehreren Primzahlen zusammengesetzten Moduls kann beinahe alles, was auf die Reste der Potenzen Bezug hat, aus der allgemeinen Theorie der Congruenzen abgeleitet werden. Da wir aber weiter unten weitläufiger zeigen werden, wie man beliebige Congruenzen nach einem aus mehreren Primzahlen zusammengesetzten Modul auf Congruenzen, deren Modul eine Primzahl oder eine Potenz einer Primzahl ist, reducieren

kann, brauchen wir uns hier mit diesem Gegenstande nicht lange aufzuhalten. Wir bemerken nur, dass die schöne Eigenschaft, welche für die andern Moduln gilt, nämlich dass es stets Zahlen giebt, deren Periode sämtliche zum Modul prime Zahlen enthält, hier nicht stattfindet, den einen Fall ausgenommen, wo der Modul das Doppelte einer Primzahl oder einer Potenz einer Primzahl ist. Wenn nämlich der Modul m auf die Form $A^a\ B^b\ C^c \dots$, wo $A, B, C, \dots$ verschiedene Primzahlen bezeichnen, gebracht, ferner $A^{a-1}(A-1)$ mit α, $B^{b-1}(B-1)$ mit β, u. s. w. bezeichnet wird und schliesslich z eine zu m prime Zahl ist, so wird $z^\alpha \equiv 1$ (mod. A^a), $z^\beta \equiv 1$ (mod. B^b), u. s. w. Wenn nun μ das kleinste gemeinschaftliche Vielfache der Zahlen $\alpha, \beta, \gamma, \dots$ ist, so wird $z^\mu \equiv 1$ nach allen Moduln A^a, $B^b, \dots$ und daher auch nach dem Modul m, welcher das Product aus jenen ist. Ausgenommen aber den Fall, wo m das Doppelte einer Primzahl oder einer Potenz einer Primzahl ist, ist der kleinste gemeinschaftliche Dividuus der Zahlen $\alpha, \beta, \gamma, \dots$ kleiner als das Product derselben (da die Zahlen $\alpha, \beta, \gamma, \dots$ nicht prim zu einander sein können, sondern wenigstens den gemeinschaftlichen Teiler 2 haben). Demnach kann von keiner Zahl die Periode soviel Glieder enthalten, als es Zahlen giebt, die prim zum Modul und kleiner als dieser sind, da deren Anzahl gleich dem Product der Zahlen $\alpha, \beta, \gamma, \dots$ ist. So ist z. B. für $m = 1001$ die sechzigste Potenz einer jeden zu m primen Zahl der Einheit congruent, weil 60 der kleinste gemeinschaftliche Dividuus der Zahlen 6, 10, 12 ist. — Der Fall aber, wo der Modul das Doppelte einer Primzahl oder der Potenz einer Primzahl ist, ist jenem, wo der Modul eine Primzahl oder die Potenz einer solchen ist, vollkommen analog.

93.

Die Schriften, in denen andere Geometer den in diesem Abschnitte dargelegten Gegenstand behandelt haben, haben wir bereits vorübergehend erwähnt. Diejenigen aber, welche einiges weitläufiger als es uns hier der Wunsch nach Kürze gestattete, behandelt sehen möchten, verweisen wir insbesondere auf die folgenden Abhandlungen Euler's, die wegen der Klarheit, durch die sich dieser grosse Mann stets vor allen andern auszeichnete, besonders empfehlenswert sind:

Theoremata circa residua ex divisione potestatum relicta. Comm. nov. Petr. T. VII p. 49.

Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia, Ibid. T. XVIII p. 85.

Auch kann man die Abhandlungen 5 und 8 in seinen *Opusculis analyticis T. I* hinzunehmen.

Vierter Abschnitt.

Von den Congruenzen zweiten Grades.



Quadratische Reste und Nichtreste.

94.

Satz. Nimmt man irgend eine Zahl m zum Modul, so können von den Zahlen 0, 1, 2, 3, ..., $m-1$, wenn m gerade ist, nicht mehr als $\frac{1}{2}m+1$, und wenn m ungerade ist, nicht mehr als $\frac{1}{2}m+\frac{1}{2}$ einem Quadrate congruent werden.

Beweis. Da die Quadrate congruenter Zahlen ebenfalls congruent sind, so wird jede Zahl, welche irgend einem Quadrate congruent werden kann, auch einem Quadrate, dessen Wurzel kleiner als m ist, congruent sein. Wir brauchen daher nur die kleinsten Reste der Quadrate 0, 1, 4, 9, ..., $(m-1)^2$ zu betrachten. Man sieht aber leicht, dass $(m-1)^2 \equiv 1$, $(m-2)^2 \equiv 2^2$, $(m-3)^2 \equiv 3^2$, u. s. w. ist. Daher werden auch, wenn m gerade ist, die kleinsten Reste der Quadrate $(\frac{1}{2}m-1)^2$ und $(\frac{1}{2}m+1)^2$, $(\frac{1}{2}m-2)^2$ und $(\frac{1}{2}m+2)^2$ u. s. w. dieselben sein; wenn aber m ungerade ist, so werden die Quadrate $(\frac{1}{2}m-\frac{1}{2})^2$ und $(\frac{1}{2}m+\frac{1}{2})^2$, $(\frac{1}{2}m-\frac{3}{2})^2$ und $(\frac{1}{2}m+\frac{3}{2})^2$ u. s. w. congruent sein. Daraus geht hervor, dass andere Zahlen als die, welche einem der Quadrate 0, 1, 4, 9, ..., $(\frac{1}{2}m)^2$ congruent sind, bei geradem m einem Quadrate nicht congruent werden können, bei ungeradem m aber jede Zahl, welche einem Quadrate congruent ist, notwendig irgend einem der folgenden 0, 1, 4, 9, ..., $(\frac{1}{2}m-\frac{1}{2})^2$ congruent ist. Daher giebt es im ersten Falle höchstens $\frac{1}{2}m+1$, im zweiten höchstens $\frac{1}{2}m+\frac{1}{2}$ verschiedene kleinste Reste.

Beispiel. Nach dem Modul 13 findet man für die Quadrate der Zahlen 0, 1, 2, 3, ..., 6 die kleinsten Reste 0, 1, 4, 9, 3, 12, 10; nach diesen kehren sie aber in umgekehrter Reihenfolge wieder. Daher kann keine Zahl, welche nicht einem von diesen Resten congruent ist, oder keine Zahl, welche einem von den folgenden 2, 5, 6, 7, 8, 11 congruent ist, einem Quadrate congruent sein.

Nach dem Modul 15 findet man folgende Reste: 0, 1, 4, 9, 1, 10, 6, 4; hiernach kehren dieselben in umgekehrter Reihenfolge wieder. Hier ist also die Anzahl der Reste, welche einem Quadrate congruent werden können, noch kleiner als $\frac{1}{2}m + \frac{1}{2}$, da dieselben 0, 1, 4, 6, 9, 10 sind. Die Zahlen 2, 3, 5, 7, 8, 11, 12, 13, 14 aber und diejenigen, welche einer von diesen congruent sind, können keinem Quadrate nach dem Modul 15 congruent werden.

95.

Hieraus folgt, dass für jeden beliebigen Modul sämtliche Zahlen in zwei Klassen verteilt werden können, von denen die eine alle Zahlen, die irgend einem Quadrate congruent werden können, die andere diejenigen, bei denen dies nicht möglich ist, enthält. Jene werden wir **quadratische Reste** der als Modul genommenen Zahl*), diese aber **quadratische Nichtreste** derselben nennen, oder werden uns auch, sobald keine Zweideutigkeit daraus entstehen kann, einfach der Ausdrücke „**Reste** und **Nichtreste**“ bedienen. Offenbar reicht es übrigens aus, wenn alle Zahlen 0, 1, 2, ..., $m - 1$ in die beiden Klassen gebracht sind, da congruente Zahlen zu derselben Klasse zu rechnen sind.

Auch bei dieser Untersuchung werden wir mit Primzahlmoduln beginnen; dies wird man also immer stillschweigend anzunehmen haben, auch wenn nicht ausdrücklich daran erinnert wird. Die Primzahl 2 ist aber auszuschliessen, oder es sind nur ungerade Primzahlen zu betrachten.

So oft der Modul eine Primzahl ist, ist die Anzahl der Reste, welche kleiner als derselbe sind, gleich der Anzahl der Nichtreste.

96.

Nimmt man eine Primzahl p zum Modul, so sind von den Zahlen $1, 2, 3, \ldots, p-1$ die Hälfte quadratische Reste, die übrigen Nichtreste, d. h. es giebt $\frac{1}{2}(p-1)$ Reste und ebensoviele Nichtreste.

Man zeigt nämlich leicht, dass alle Quadrate $1, 4, 9, \ldots, \frac{1}{4}(p-1)^2$ einander incongruent sind. Denn wenn $r^2 \equiv r'^2$ (mod. p) werden könnte und die Zahlen r und r' von einander verschieden und nicht grösser als $\frac{1}{2}(p-1)$

*) Eigentlich bedienen wir uns hier dieses Ausdrucks in einem andern Sinne, als wir es bisher gethan haben. Wir müssten nämlich sagen, r sei Rest des Quadrates a^2 nach dem Modul m, wenn $r \equiv a^2$ (mod. m) ist. Der Kürze wegen werden wir aber in diesem Abschnitt stets r den quadratischen Rest von m selbst nennen und haben nicht zu befürchten, dass hieraus irgend eine Zweideutigkeit entstehen wird. Denn den Ausdruck Rest werden wir, wenn er dasselbe bezeichnet wie congruente Zahl, von nun an nur anwenden, wenn von kleinsten Resten die Rede ist, wobei kein Zweifel entstehen kann.

wären, so würde, wenn man $r > r'$ annimmt, was erlaubt ist, $(r - r')(r + r')$ positiv und durch p teilbar sein. Nun ist aber jeder der beiden Factoren $r - r'$ und $r + r'$ kleiner als p, somit kann unsre Annahme nicht stattfinden (Artikel 13). Es giebt daher $\frac{1}{2}(p - 1)$ quadratische Reste unter den Zahlen $1, 2, 3, \ldots, p - 1$; mehr aber kann es unter ihnen nicht geben, weil mit Hinzurechnung des Restes 0 sich $\frac{1}{2}(p + 1)$ ergeben, welche Zahl die Anzahl aller Reste nicht übersteigen kann. Daher werden die übrigen Zahlen Nichtreste und deren Anzahl somit gleich $\frac{1}{2}(p - 1)$ sein.

Da die Null immer Rest ist, so werden wir diese sowie die durch den Modul teilbaren Zahlen von diesen Untersuchungen ausschliessen, weil dieser Fall von selbst klar ist und die Kürze der Sätze nur stören würde. Aus demselben Grunde haben wir auch den Modul 2 ausgeschlossen.

97.

Da mehreres, was wir in diesem Abschnitt auseinandersetzen werden, auch aus den Prinzipien des vorigen Abschnitts abgeleitet werden kann, und es nicht unnützlich ist, eine und dieselbe Wahrheit auf verschiedenen Wegen zu ermitteln, so wollen wir diesen Zusammenhang klarlegen. Man sieht aber leicht ein, dass alle einem Quadrate congruente Zahlen gerade Indices, diejenigen aber, welche einem Quadrate in keiner Weise congruent werden können, ungerade Indices haben. Da nun $p - 1$ eine gerade Zahl ist, so wird es gleichviel gerade und ungerade Indices, nämlich von jeder Art $\frac{1}{2}(p - 1)$, und ebensoviele Reste und Nichtreste geben.

Beispiele. Für die Moduln sind Reste

Für die Moduln	sind Reste
3	1
5	1, 4
7	1, 2, 4
11	1, 3, 4, 5, 9
13	1, 3, 4, 9, 10, 12
17	1, 2, 4, 8, 9, 13, 15, 16
. . . . . .	. . . .;

die übrigen Zahlen aber, welche kleiner als diese Moduln sind, sind Nichtreste.

Die Antwort auf die Frage, ob eine zusammengesetzte Zahl Rest oder Nichtrest einer gegebenen Primzahl sei, hängt von der Natur der Factoren ab.

98.

Satz. Das Product aus zwei quadratischen Resten der Primzahl p ist ein Rest; das Product aus einem Rest und einem Nichtrest ist ein Nichtrest; endlich das Product aus zwei Nichtresten ist ein Rest.

Beweis. I. Sind A, B die aus den Quadraten a^2, b^2 entstehenden Reste oder also $A \equiv a^2$, $B \equiv b^2$, so wird das Product AB dem Quadrate der Zahl ab congruent also ein Rest.

II. Ist A ein Rest, etwa $\equiv a^2$, B dagegen ein Nichtrest, so wird AB ein Nichtrest. Denn setzt man, wenn dies möglich ist, $AB \equiv k^2$ und ist der Wert des Ausdrucks $\frac{k}{a}$ (mod. p) $\equiv b$, so wird $a^2 B \equiv a^2 b^2$, daher $B \equiv b^2$, d. h. B wird unserer Voraussetzung entgegen ein Rest.

Andrer Beweis. Multipliciert man alle unter den Zahlen 1, 2, 3, ..., $p-1$ enthaltenen Reste (deren Anzahl gleich $\frac{1}{2}(p-1)$ ist) mit A, so werden alle Producte quadratische Reste und zwar sämtlich einander incongruent sein. Multipliciert man nun den Nichtrest B mit A, so wird das Product keinem der bereits erhaltenen Producte congruent sein. Wäre es daher ein Rest, so würde man $\frac{1}{2}(p+1)$ incongruente Reste haben, unter denen der Rest 0 sich noch nicht befände. Dies widerspricht aber dem Artikel 96.

III. Sind A und B Nichtreste und multipliciert man alle unter den Zahlen 1, 2, 3, ..., $p-1$ vorkommenden Reste mit A, so erhält man nach II. $\frac{1}{2}(p-1)$ einander incongruente Nichtreste. Nun kann aber das Product AB keinem von diesen congruent sein. Wenn es also ein Nichtrest wäre, so hätte man $\frac{1}{2}(p+1)$ einander incongruente Nichtreste, was dem Artikel 96 widerspricht. Daher u. s. w.

Leichter noch kann man diese Sätze aus den Prinzipien des vorigen Abschnittes ableiten. Denn weil die Indices der Reste stets gerade, die der Nichtreste aber stets ungerade sind, so wird der Index des Products zweier Reste oder Nichtreste gerade und daher das Product selbst ein Rest. Dagegen wird der Index des Products aus einem Rest und einem Nichtrest ungerade und daher das Product selbst ein Nichtrest.

Beide Beweismethoden können auch auf folgende Sätze angewendet werden:

Der Wert des Ausdrucks $\frac{a}{b}$ (mod. p) ist ein Rest, wenn die Zahlen a und b gleichzeitig Reste oder Nichtreste sind; derselbe wird aber ein Nichtrest sein, wenn von den Zahlen a und b die eine ein Rest, die andere ein Nichtrest ist.

Diese Sätze lassen sich auch durch Umkehrung der vorhergehenden Sätze erhalten.

99.

Allgemein ist das Product aus beliebig vielen Factoren ein Rest, sowohl wenn dieselben sämtlich Reste sind als auch wenn die Anzahl der unter ihnen vorkommenden Nichtreste gerade ist; wenn aber die Anzahl der Nichtreste, welche sich unter den Factoren vorfinden, ungerade ist, so ist das

Product ein Nichtrest. Man kann daher leicht entscheiden, ob eine gegebene Zahl Rest ist oder nicht, wenn man nur weiss, was die einzelnen Factoren desselben sind. Wir haben daher in die Tafel II nur die Primzahlen aufgenommen. Die Einrichtung dieser Tafel ist folgende. Am Rande stehen die Moduln*), am Kopfe der Seite aber die aufeinanderfolgenden Primzahlen; so oft irgend eine von diesen Rest eines Moduls ist, ist in den beiden gleichzeitig zugehörigen Raum ein kleiner Strich gesetzt worden; wenn aber die Primzahl Nichtrest des Moduls ist, ist der betreffende Raum leer geblieben.

Über Moduln, welche zusammengesetzte Zahlen sind.

100.

Bevor wir zu schwierigeren Sachen übergehen, müssen wir noch Einiges über nicht prime Moduln hinzufügen.

Wenn eine beliebige Potenz p^n der Primzahl p (wo wir annehmen, dass p nicht gleich 2 sei) zum Modul genommen wird, so sind die eine Hälfte aller Zahlen, welche durch p nicht teilbar und kleiner als der Modul sind; Reste, die andere Nichtreste, d. h. die Anzahl der einen und der andern ist gleich $\frac{1}{2}(p-1)\,p^{n-1}$.

Wenn nämlich r ein Rest ist, so wird er irgend einem Quadrate congruent sein, dessen Wurzel die Hälfte des Moduls nicht übersteigt. (Vgl. Artikel 94). Nun sieht man leicht, dass es $\frac{1}{2}(p-1)p^{n-1}$ Zahlen giebt, welche durch p nicht teilbar und kleiner als die Hälfte des Moduls sind, man hat daher nur zu zeigen, dass die Quadrate aller dieser Zahlen einander incongruent sind oder verschiedene quadratische Reste ergeben. Wenn nun die Quadrate zweier Zahlen a und b, die durch p nicht teilbar und kleiner als die Hälfte des Moduls sind, congruent wären, so müsste $a^2 - b^2$ oder $(a-b)\;(a+b)$ durch p^n teilbar sein (wenn man, was erlaubt ist, annimmt, dass $a > b$ sei). Dies wäre aber nur möglich, wenn entweder die eine der Zahlen $a-b$, $a+b$ durch p^n teilbar wäre, was nicht der Fall sein kann, weil beide kleiner als p^n sind, oder wenn die eine durch p^m, die andere durch p^{n-m} d. h. beide durch p sich teilen liessen. Aber auch dies ist nicht möglich. Denn offenbar würde dann auch die Summe und Differenz derselben nämlich $2a$, $2b$ durch p und somit auch a und b durch p teilbar sein, was der Voraussetzung widerspricht. Hieraus folgt schliesslich, dass es unter den Zahlen, welche durch p nicht teilbar und kleiner als der Modul sind, $\frac{1}{2}\;(p-1)\;p^{n-1}$ Reste giebt und dass die übrigen, deren Anzahl gleich gross ist, Nichtreste sind. — Man könnte diesen Satz auch nach Analogie von Artikel 97 aus der Betrachtung der Indices ableiten.

---

*) Wie wir uns auch von den zusammengesetzten Moduln freimachen können, werden wir bald zeigen.

101.

Jede durch p nicht teilbare Zahl, welche Rest von p ist, ist auch Rest von p^n und die, welche Nichtrest ist von p, ist auch Nichtrest von p^n.

Der letzte Teil dieses Satzes ist an sich klar. Wenn daher der erste Teil unrichtig wäre, so würde es unter den Zahlen, welche kleiner als p^n und zugleich durch p nicht teilbar wären, mehr Reste von p als von p^n, d. h. mehr als $\frac{1}{2}p^{n-1}(p-1)$ geben. Man sieht aber ohne Schwierigkeit, dass die Anzahl der Reste der Zahl p unter jenen Zahlen genau gleich $\frac{1}{2}p^{n-1}(p-1)$ ist.

Ebenso leicht ist es, ein Quadrat wirklich zu finden, welches nach dem Modul p^n einem gegebenen Reste congruent ist, wenn man ein diesem Reste nach dem Modul p congruentes Quadrat hat.

Wenn man nämlich ein Quadrat hat, a^2, welches einem gegebenen Reste A nach dem Modul p^μ congruent ist, so leitet man daraus ein dem Reste A nach dem Modul p^ν (wo $\nu > \mu$ aber $\overline{\overline{<}}\, 2\mu$ vorausgesetzt wird) congruentes Quadrat auf folgende Weise her. Man setze die Wurzel des gesuchten Quadrates gleich $\pm a + xp^\mu$, welche Form dieselbe, wie man leicht sieht, haben muss. Dann soll sein: $a^2 \pm 2axp^\mu + x^2p^{2\mu} \equiv A \pmod{p^\nu}$, oder, da $2\mu > \nu$ ist, $A - a^2 \equiv \pm 2axp^\mu \pmod{p^\nu}$. Ist $A - a^2 = p^\mu d$, so ist x der Wert des Ausdrucks $\pm \frac{d}{2a} \pmod{p^{\nu-\mu}}$, welcher dem Ausdruck $\pm \frac{A-a^2}{2ap^\mu}$ $\pmod{p^\nu}$ äquivalent ist.

Ist also ein Quadrat gegeben, welches A nach dem Modul p congruent ist, so leitet man daraus ein Quadrat ab, welches A nach dem Modul p^2 congruent ist; von hier kann man dann zum Modul p^4, sodann zum Modul p^8 u. s. w. aufsteigen.

Beispiel. Ist der Rest 6, welcher nach dem Modul 5 dem Quadrate 1 congruent ist, gegeben, so findet man das Quadrat 9^2, welchem er nach dem Modul 25 congruent ist, ferner das Quadrat 16^2, welchem er nach dem Modul 125 congruent ist, u. s. w.

102.

Was aber die durch p teilbaren Zahlen anlangt, so ist klar, dass deren Quadrate durch p^2 teilbar sein werden, und dass daher alle zwar durch p aber nicht durch p^2 teilbaren Zahlen Nichtreste von p^n sind. Allgemein aber sind, wenn eine Zahl p^kA, wo A durch p nicht teilbar ist, gegeben ist, folgende Fälle zu unterscheiden:

1. Ist $k \overline{\overline{>}}\, n$, so ist $p^kA \equiv 0 \pmod{p^n}$, d. h. die gegebene Zahl ist ein Rest.

2. Ist $k < n$ und ungerade, so ist p^kA ein Nichtrest.

Wenn nämlich $p^kA = p^{2\varkappa+1}A \equiv s^2 \pmod{p^n}$ wäre, so würde s^2 durch $p^{2\varkappa+1}$ teilbar sein, und dies könnte nur der Fall sein, wenn s durch $p^{\varkappa+1}$ teilbar wäre. Dann würde aber s^2 auch durch $p^{2\varkappa+2}$ und somit auch (da

$2\varkappa+2$ sicher nicht grösser als n ist) $p^k A$ d. i. $p^{2\varkappa+1}A$ durch dieses teilbar sein, oder es würde A durch p sich teilen lassen müssen, was der Voraussetzung widerspricht.

3. k ist kleiner als n und gerade. Dann wird $p^k A$ ein Rest oder Nichtrest von p^n sein, je nachdem A Rest oder Nichtrest von p ist. Denn wenn A Rest ist von p, so wird es auch Rest von p^{n-k}. Setzt man aber $A \equiv a^2$ (mod. p^{n-k}), so wird $Ap^k \equiv a^2 p^k$ (mod. p^n) und $a^2 p^k$ ist ein Quadrat. Wenn dagegen A Nichtrest von p ist, so kann $p^k A$ nicht Rest von p^n sein. Denn setzte man $p^k A \equiv a^2$ (mod. p^n), so würde notwendig a^2 durch p^k teilbar sein müssen. Der Quotient würde ein Quadrat sein, welchem A nach dem Modul p^{n-k} und daher auch nach dem Modul p congruent wäre, d. h. A würde Rest von p sein. Dies widerspricht aber der Voraussetzung.

103.

Da wir den Fall $p=2$ ausgeschlossen haben, müssen wir über diesen noch einiges hinzufügen. Ist die Zahl 2 der Modul, so ist jede Zahl Rest; Nichtreste giebt es nicht. Ist aber 4 der Modul, so werden alle ungeraden Zahlen von der Form $4k+1$ Reste, alle Zahlen aber von der Form $4k+3$ Nichtreste sein. Ist endlich 8 oder eine höhere Potenz von 2 der Modul, so werden alle ungeraden Zahlen von der Form $8k+1$ Reste, alle andern aber oder alle diejenigen, welche von einer der Formen $8k+3$, $8k+5$, $8k+7$ sind, Nichtreste sein. Der letzte Teil dieses Satzes erhellt daraus, dass das Quadrat einer jeden ungeraden Zahl, mag dieselbe von der Form $4k+1$ oder von der Form $4k-1$ sein, von der Form $8k+1$ wird. Den ersten Teil beweisen wir folgendermassen.

1. Wenn die Summe oder Differenz zweier Zahlen durch 2^{n-1} teilbar ist, so sind die Quadrate der Zahlen nach dem Modul 2^n congruent. Denn wenn die eine gleich a gesetzt wird, so ist die andere von der Form $2^{n-1}h \pm a$, und das Quadrat dieser findet man $\equiv a^2$ (mod. 2^n).

2. Jede ungerade Zahl, welche quadratischer Rest von 2^n ist, wird einem Quadrate congruent sein, dessen Wurzel eine ungerade Zahl und kleiner als 2^{n-2} ist. Es sei nämlich a^2 irgend ein Quadrat, welchem jene Zahl congruent ist, und die Zahl $a \equiv \pm \alpha$ (mod. 2^{n-1}), so dass α die Hälfte des Moduls nicht übersteigt (Artikel 4); dann ist $a^2 \equiv \alpha^2$. Somit ist auch die gegebene Zahl $\equiv \alpha^2$. Offenbar werden dann sowohl a als α ungerade und $\alpha < 2^{n-2}$ sein.

3. Die Quadrate aller ungeraden Zahlen, die kleiner als 2^{n-2} sind, sind nach dem Modul 2^n incongruent. Es seien nämlich r und s zwei solche Zahlen. Wären deren Quadrate nach dem Modul 2^n congruent, so würde $(r-s)(r+s)$ durch 2^n teilbar sein (wo $r > s$ angenommen ist). Man sieht aber leicht, dass die Zahlen $r-s$ und $r+s$ zu gleicher Zeit nicht durch 4 teilbar sein können, daher muss, wenn die eine nur durch 2 teilbar ist, die andere durch 2^{n-1} teilbar sein, damit das Product durch 2^n teilbar werde. Dies ist aber absurd, da jede der beiden Zahlen kleiner als 2^{n-2} ist.

4. Wenn nun endlich diese Quadrate auf ihre kleinsten positiven Reste reduciert werden, so erhält man 2^{n-3} von einander verschiedene quadratische Reste, welche kleiner als der Modul sind*) und von denen jeder von der Form $8k+1$ sein wird. Da es aber genau 2^{n-3} Zahlen von der Form $8k+1$, welche kleiner als der Modul sind, giebt, so müssen sich diese notwendig sämtlich unter jenen Resten vorfinden. Dies sollte aber bewiesen werden.

Um ein einer gegebenen Zahl von der Form $8k+1$ nach dem Modul 2^n congruentes Quadrat zu finden, kann man ein analoges Verfahren einschlagen wie in Artikel 101. Man vergleiche auch Artikel 88. — Schliesslich gilt von den geraden Zahlen dasselbe, was wir im Artikel 102 allgemein auseinandergesetzt haben.

104.

Hinsichtlich der Anzahl der verschiedenen (d. h. nach dem Modul incongruenten) Werte, welche der Ausdruck $V = \sqrt{A} \pmod{p^n}$ besitzt, wenn A Rest von p^n ist, kann man aus dem Vorhergehenden leicht Folgendes ableiten. (Die Zahl p setzen wir, wie vorher, als Primzahl voraus und schliessen der Kürze wegen den Fall $n=1$ sogleich aus.)

I. Wenn A durch p nicht teilbar ist, so hat V einen Wert für $p=2$, $n=1$, nämlich $V\equiv 1$; zwei Werte, wenn p ungerade ist, sowie auch für $p=2$, $n=2$; es wird nämlich, wenn man den einen $\equiv v$ setzt, der andere $\equiv -v$ sein; vier Werte für $p=2$, $n>2$; es sind nämlich, wenn man den einen $\equiv v$ setzt, die übrigen $\equiv -v$, $2^{n-1}+v$, $2^{n-1}-v$.

II. Wenn A durch p aber nicht durch p^n teilbar ist, so sei die höchste Potenz von p, welche in A aufgeht, $p^{2\mu}$ (offenbar nämlich wird der Exponent derselbe gerade sein müssen) und $A = ap^{2\mu}$. Dann ist klar, dass alle Werte von V durch p^μ teilbar sind und alle aus der Division hervorgehenden Quotienten Werte des Ausdrucks $V' = \sqrt{a} \pmod{p^{n-2\mu}}$ werden. Aus diesen wird man alle verschiedenen Werte von V erhalten, wenn man alle zwischen 0 und $p^{n-\mu}$ gelegenen Werte des Ausdruckes V' mit p^μ multipliciert. Daher werden jene dargestellt durch

$$vp^\mu,\ vp^\mu + p^{n-\mu},\ vp^\mu + 2p^{n-\mu},\ \ldots,\ vp^\mu + (p^\mu - 1)p^{n-\mu},$$

wenn v unbestimmt alle verschiedenen Werte des Ausdrucks V' ausdrückt, so dass die Anzahl jener gleich p^μ, $2p^\mu$ oder $4p^\mu$ wird, je nachdem die Anzahl dieser (nach Fall I) gleich 1, 2 oder 4 ist.

III. Ist A durch p^n teilbar, so sieht man leicht, dass, wenn man $n=2m$ oder $=2m-1$ setzt, je nachdem es gerade oder ungerade ist, alle durch p^m teilbaren Zahlen, und keine andern, Werte von V sind. Daher sind 0, p^m, $2p^m$, $\ldots$, $(p^{n-m}-1)p^m$ sämtliche von einander verschiedene Werte, und die Anzahl dieser ist gleich p^{n-m}.

*) Da nämlich die Anzahl der ungeraden Zahlen unterhalb 2^{n-2} gleich 2^{n-3} ist.

105.

Es bleibt der Fall übrig, wo der Modul m aus mehreren Primzahlen zusammengesetzt ist. Ist $m = abc\ldots$, wo $a, b, c, \ldots$ von einander verschiedene Primzahlen oder Potenzen verschiedener Primzahlen bezeichnen, so ist sofort klar, dass, wenn n ein Rest von m ist, auch n Rest der einzelnen $a, b, c, \ldots$ sein wird, und dass daher sicher n Nichtrest von m ist, wenn es ein Nichtrest irgend einer der Zahlen $a, b, c, \ldots$ ist. Umgekehrt wird n, wenn es Rest der einzelnen Zahlen $a, b, c, \ldots$ ist, auch Rest des Productes sein. Denn setzt man $n \equiv A^2, B^2, C^2, \ldots$ respective nach den Moduln $a, b, c, \ldots$, so wird offenbar, wenn man nach Artikel 32 eine Zahl N abgeleitet hat, welche $A, B, C, \ldots$ respective nach den Moduln $a, b, c, \ldots$ congruent ist, $n \equiv N^2$ nach allen diesen Moduln und daher auch nach dem Producte m sein. — Da man leicht sieht, dass auf diese Weise aus der Combination jedes Wertes von A oder des Ausdrucks $\sqrt{n}$ (mod. a) mit jedem Werte von B mit jedem Werte von C u. s. w. ein Wert von N oder des Ausdrucks $\sqrt{n}$ (mod. m) entsteht, sowie ferner, dass aus verschiedenen Combinationen verschiedene N und aus allen sämtliche N hervorgehen, so ist die Anzahl sämtlicher verschiedenen Werte von N gleich dem Producte aus den Anzahlen der Werte von $A, B, C, \ldots$, die wir im vorigen Artikel zu bestimmen gelehrt haben. — Ferner ist klar, dass, wenn ein Wert des Ausdrucks $\sqrt{n}$ (mod. m) oder von N bekannt ist, dieser zugleich ein Wert aller $A, B, C, \ldots$ sein wird, und da aus diesem nach dem vorigen Artikel alle übrigen Werte dieser Grössen abgeleitet werden können, so folgt leicht, dass man aus einem Werte von N alle übrigen erhalten kann.

Beispiel. Der Modul sei 315; es wird gefragt, ob 46 Rest oder Nichtrest desselben sei. Die Primteiler der Zahl 315 sind 3, 5, 7, und die Zahl 46 ist Rest eines jeden derselben und daher auch Rest von 315. Da ferner $46 \equiv 1$ und $\equiv 64$ nach dem Modul 9, $\equiv 1$ und $\equiv 16$ nach dem Modul 5, $\equiv 4$ und $\equiv 25$ nach dem Modul 7 ist, so findet man als Wurzeln der Quadrate, denen 46 nach dem Modul 315 congruent ist, folgende Zahlen: 19, 26, 44, 89, 226, 271, 289, 296.

Allgemeines Kriterium dafür, dass eine gegebene Zahl Rest oder Nichtrest einer gegebenen Primzahl ist.

106.

Aus dem Vorhergehenden folgt, dass, wenn man nur in jedem Falle entscheiden kann, ob eine gegebene Primzahl Rest oder Nichtrest einer gegebenen Primzahl ist, alle übrigen Fälle auf diesen sich zurückführen lassen. Wir müssen daher unsere Bemühungen darauf richten, für jenen Fall sichere Kriterien zu ermitteln. Bevor wir aber diese Untersuchung in Angriff nehmen, wollen wir ein gewisses aus dem vorigen Abschnitte sich

ergebendes Kriterium anführen, dass zwar in der Praxis fast gar keine Anwendung findet, aber wegen seiner Einfachheit und Allgemeinheit erwähnenswert ist.

Jede beliebige Zahl A, welche durch die Primzahl $2m+1$ nicht teilbar ist, ist Rest oder Nichtrest dieser Primzahl, je nachdem $A^m \equiv +1$ oder $\equiv -1 \pmod{2m+1}$ ist.

Ist nämlich für den Modul $2m+1$ in einem beliebigen Systeme der Index der Zahl A gleich a, so wird a gerade sein, wenn A Rest von $2m+1$ ist, dagegen ungerade, wenn A Nichtrest ist. Der Index der Zahl A^m ist aber ma, d. h. er ist $\equiv 0$ oder $\equiv m \pmod{2m}$, je nachdem a gerade oder ungerade ist. Hieraus wird schliesslich in dem ersteren Falle $A^m \equiv +1$, im letzteren dagegen $A^m \equiv -1 \pmod{2m+1}$. Vgl. Artikel 57 und 62.

Beispiel. 3 ist Rest von 13, weil $3^6 \equiv 1 \pmod{13}$ ist; dagegen ist 2 Nichtrest von 13, weil $2^6 \equiv -1 \pmod{13}$ ist.

Sobald aber die zu untersuchenden Zahlen auch nur mässig gross sind, wird dieses Kriterium wegen der Weitläufigkeit der Rechnung völlig unbrauchbar.

Untersuchungen über die Primzahlen, deren Reste oder Nichtreste gegebene Zahlen sind.

107.

Es ist zwar sehr leicht, für einen gegebenen Modul alle Zahlen anzugeben, welche Reste oder Nichtreste desselben sind. Denn wenn jene Zahl $= m$ gesetzt wird, so muss man die Quadrate bestimmen, deren Wurzeln die Hälfte von m nicht übersteigen, oder auch Zahlen, welche diesen Quadraten nach m congruent sind (für die Praxis giebt es noch bequemere Methoden), und dann werden alle Zahlen, welche irgend einem von diesen nach m congruent sind, Reste, alle Zahlen aber, welche keinem von ihnen congruent sind, Nichtreste von m sein. — Aber die umgekehrte **Aufgabe**: Wenn irgend eine Zahl gegeben ist, alle Zahlen zu bestimmen, von denen jene Rest oder Nichtrest ist, ist bedeutend schwieriger. Dieses Problem, von dessen Lösung dasjenige, welches wir uns im vorigen Artikel vorgenommen haben, abhängt, wollen wir im Folgenden behandeln und fangen dabei mit den einfachsten Fällen an.

Der Rest -1.

108.

Satz. Von allen Primzahlen von der Form $4n+1$ ist -1 quadratischer Rest, dagegen Nichtrest von allen Primzahlen von der Form $4n+3$.

Beispiel. — 1 ist Rest der Zahlen 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, ... und ergiebt sich respective aus den Quadraten der Zahlen 2, 5, 4, 12, 6, 9, 23, 11, 27, 34, 22, ...; dagegen Nichtrest der Zahlen 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, ...

Diesen Satz haben wir schon in Artikel 64 erwähnt. Der Beweis aber ergiebt sich leicht aus Artikel 106. Denn für eine Primzahl von der Form $4n+1$ ist $(-1)^{2n} \equiv 1$, für eine Primzahl aber von der Form $4n+3$ hat man $(-1)^{2n+1} \equiv -1$. Dieser Beweis stimmt mit dem am erwähnten Orte angeführten überein. Wegen der Eleganz und der Brauchbarkeit des Satzes wird es jedoch nicht überflüssig sein, denselben noch auf eine andere Art zu beweisen.

109.

Den Complex aller Reste der Primzahl p, welche kleiner sind als p, mit Ausschluss des Restes 0 wollen wir mit dem Buchstaben C bezeichnen. Da die Anzahl dieser Reste stets gleich $\frac{p-1}{2}$ ist, so ist dieselbe offenbar gerade, wenn p von der Form $4n+1$, dagegen ungerade, wenn p von der Form $4n+3$ ist. Nach Analogie des Artikel 77, wo von den Zahlen im Allgemeinen gehandelt wurde, mögen solche Reste, deren Product $\equiv 1 \pmod{p}$ ist, **associierte** Reste genannt werden; denn offenbar wird, wenn r ein Rest ist, auch $\frac{1}{r} \pmod{p}$ Rest sein. Da nun ein und derselbe Rest mehrere associierte Reste unter den Resten C nicht haben kann, so leuchtet ein, dass alle Reste C in Klassen verteilt werden können, deren jede je zwei associierte Reste enthält. Nun ist klar, dass, wenn es keinen sich selbst associierten Rest gäbe, d. h. wenn jede Klasse je zwei ungleiche Reste enthielte, die Anzahl aller Reste das Doppelte der Anzahl aller Klassen sein würde. Giebt es dagegen irgend welche sich selbst associierte Reste, d. h. etliche Klassen, welche nur einen einzigen Rest, oder, wenn man lieber will, denselben Rest zweimal enthalten, und setzt man die Anzahl dieser Klassen gleich a, die der übrigen gleich b, so wird die Anzahl aller Reste C gleich $a+2b$ sein. Ist daher p von der Form $4n+1$, so ist a eine gerade Zahl; ist dagegen p von der Form $4n+3$, so ist a ungerade. Andere Zahlen aber, als 1 und $p-1$, welche kleiner als p sind, können sich nicht selbst associiert sein (Vgl. Artikel 77), und die erstere 1 kommt sicher unter den Resten vor. Daher muss im ersteren Falle $p-1$ (oder, was hier dasselbe ist, -1) Rest, im letzteren aber Nichtrest sein, denn sonst würde in jenem Falle $a=1$, in diesem aber $a=2$ sein, was nicht möglich ist.

110.

Auch dieser Beweis rührt von Euler her, der auch zuerst den ersten gefunden hat. Vgl. *Opusc. Anal. T. I. p. 135.* — Man wird leicht erkennen, dass derselbe auf ähnlichen Principien beruht, wie unser zweiter Beweis

des Wilson'schen Satzes im Artikel 77. Wenn man aber diesen Satz voraussetzen will, so kann man den Beweis noch leichter führen. Unter den Zahlen 1, 2, 3, ..., $p-1$ giebt es nämlich $\frac{p-1}{2}$ quadratische Reste von p und ebensoviele Nichtreste. Daher ist die Anzahl der Nichtreste gerade, wenn p von der Form $4n+1$, ungerade, wenn p von der Form $4n+3$ ist. Somit wird das Product aus allen Zahlen 1, 2, 3, ..., $p-1$ im ersten Falle ein Rest, im zweiten ein Nichtrest (Artikel 99). Dieses Product ist aber stets $\equiv -1 \pmod{p}$; mithin ist -1 im ersten Falle ein Rest, im zweiten ein Nichtrest.

111.

Wenn daher r Rest irgend einer Primzahl von der Form $4n+1$ ist, so wird auch $-r$ Rest dieser Primzahl sein, dagegen werden alle Nichtreste einer solchen Zahl, auch wenn sie mit dem negativen Zeichen genommen werden, Nichtreste bleiben.*) Das Gegenteil ist der Fall bei den Primzahlen von der Form $4n+3$, deren Reste zu Nichtresten werden, wenn man das Vorzeichen ändert und umgekehrt. Vgl. Artikel 98.

Übrigens leitet man aus dem Vorhergehenden leicht die **allgemeine Regel** her: -1 ist Rest aller Zahlen, welche weder durch 4 noch durch irgend eine Primzahl von der Form $4n+3$ teilbar sind, dagegen Nichtrest aller übrigen. Vgl. Artikel 103 und 105.

Reste $+2$ und -2.

112.

Wir gehen jetzt zu den Resten $+2$ und -2 weiter.

Sammeln wir aus der Tafel II alle Primzahlen, deren Rest $+2$ ist, so erhalten wir die folgenden: 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97. Man bemerkt aber leicht, dass sich unter diesen keine Zahlen von der Form $8n+3$ und $8n+5$ finden. Wir wollen daher zusehen, ob wir diesen Inductionsschluss streng begründen können.

Zunächst bemerken wir, dass jede zusammengesetzte Zahl von der Form $8n+3$ oder $8n+5$ notwendig einen Primfactor von einer der beiden Formen $8n+3$ oder $8n+5$ enthält; denn offenbar lassen sich aus lauter Primzahlen von der Form $8n+1$ und $8n+7$ keine andern Zahlen, als solche, welche von der Form $8n+1$ oder $8n+7$ sind, zusammensetzen. Wenn daher unser Inductionsschluss allgemein richtig ist, so giebt es überhaupt keine Zahl von der Form $8n+3$ oder $8n+5$, deren Rest $+2$ ist. So giebt es z. B. sicher keine Zahl von dieser Form unter 100, deren Rest

*) Wenn wir also von einer Zahl als von einem Rest oder Nichtrest einer Zahl von der Form $4n+1$ sprechen, so können wir das Vorzeichen derselben ganz weglassen oder auch ihr das doppelte Vorzeichen $\pm$ beilegen.

$+2$ ist. Wenn aber jenseits dieser Grenze solche Zahlen vorkommen sollten, so möge die kleinste von allen gleich t gesetzt werden. Es wird also t entweder von der Form $8n+3$ oder von der Form $8n+5$ sein, und $+2$ wird Rest von ihr sein, während es von allen kleineren Zahlen dieser Art Nichtrest ist. Setzt man $2 \equiv a^2$ (mod. t), so kann man a immer so annehmen, dass es ungerade und zugleich kleiner als t ist (denn es besitzt a mindestens zwei positive Werte, die kleiner als t sind und deren Summe gleich t ist, von denen somit die eine gerade, die andere ungerade ist. (Vgl. Artikel 104 und 105)). Ist dies geschehen und ist $a^2 = 2 + tu$ oder $tu = a^2 - 2$, so wird a^2 von der Form $8n+1$, tu also von der Form $8n-1$ und daher u entweder von der Form $8n+3$ oder von der Form $8n+5$ sein, je nachdem t von der letzteren oder ersteren Form ist. Aus der Gleichung $a^2 = 2 + tu$ folgt aber, dass auch $2 \equiv a^2$ (mod. u) d. h. 2 auch Rest von u ist. Man sieht jedoch leicht, dass $u < t$ ist und dass somit t im Widerspruche mit unserer Voraussetzung nicht die kleinste Zahl ist, für welche unser Inductionsschluss nicht gilt. Hieraus folgt offenbar, dass das, was wir durch Induction gefunden hatten, allgemein richtig ist.

Combinieren wir dies mit dem im Artikel 111 gefundenen Satze, so erhalten wir folgende **Sätze**:

I. Für alle Primzahlen von der Form $8n+3$ ist $+2$ Nichtrest, -2 dagegen Rest.

II. Für alle Primzahlen von der Form $8n+5$ ist sowohl $+2$ als auch -2 ein Nichtrest.

113.

Durch analoge Induction findet man aus der Tafel II die folgenden Primzahlen, deren Rest -2 ist: 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97.*) Da sich unter diesen keine von der Form $8n+5$ oder $8n+7$ vorfindet, so untersuchen wir, ob dieser Inductionsschluss die Bedeutung eines allgemeinen Satzes erhalten kann. Man zeigt auf ähnliche Weise wie im vorigen Artikel, dass jede zusammengesetzte Zahl von der Form $8n+5$ oder $8n+7$ einen Primfactor von der Form $8n+5$ oder $8n+7$ enthält, so dass, wenn unser Inductionsschluss allgemein richtig ist, -2 überhaupt von keiner Zahl von der Form $8n+5$ oder $8n+7$ Rest sein kann. Wenn es aber derartige Zahlen gäbe, so möge die kleinste von allen gleich t gesetzt und $-2 = a^2 - tu$ werden. Hierbei ist, wenn a wie oben ungerade und kleiner als t angenommen wird, u von der Form $8n+5$ oder $8n+7$, je nachdem t von der Form $8n+7$ oder $8n+5$ ist. Daraus aber, dass $a^2 + 2 = tu$ und $a < t$ ist, wird man leicht ableiten können, dass auch u kleiner als t ist. Schliesslich wird -2 auch Rest von u sein, d. h. t ist, im Widerspruche mit unserer Voraussetzung, nicht die kleinste Zahl, für welche

*) Wenn man nämlich -2 als Product aus $+2$ und -1 betrachtet. Vgl. Artikel 111.

unser Inductionsschluss nicht gilt. Daher ist notwendig -2 Nichtrest aller Zahlen von der Form $8n+5$ und $8n+7$.

Verbindet man dies mit dem Satze des Artikels 111, so ergeben sich folgende **Sätze**:

I. Von allen Primzahlen von der Form $8n+5$ ist sowohl -2 als $+2$ Nichtrest, wie wir schon im vorigen Artikel gefunden haben.

II. Von allen Primzahlen von der Form $8n+7$ ist -2 Nichtrest, $+2$ dagegen Rest.

Übrigens hätten wir in jedem der beiden Beweise für a auch einen geraden Wert nehmen können; dann hätten wir aber den Fall, wo a von der Form $4n+2$ ist, von demjenigen, wo es von der Form $4n$ ist, unterscheiden müssen. Die Entwicklung schreitet genau ebenso vorwärts wie oben und unterliegt keiner Schwierigkeit.

114.

Es bleibt noch ein Fall übrig, nämlich der, wo die Primzahl von der Form $8n+1$ ist. Bei diesem aber schlägt die vorige Methode fehl, vielmehr erfordert derselbe durchaus eigentümliche Kunstgriffe.

Ist für einen Primzahlmodul von der Form $8n+1$ eine beliebige primitive Wurzel gleich a, so ist (Artikel 62) $a^{4n} \equiv -1 \pmod{8n+1}$, welche Congruenz man auch in der Form $(a^{2n}+1)^2 \equiv 2a^{2n} \pmod{8n+1}$, oder auch in der Form $(a^{2n}-1)^2 \equiv -2a^{2n}$ darstellen kann. Hieraus folgt, dass sowohl $2a^{2n}$ als auch $-2a^{2n}$ Rest von $8n+1$ ist. Da aber a^{2n} ein durch den Modul nicht teilbares Quadrat ist, so sind offenbar $+2$ und -2 Reste (Artikel 98)*).

115.

Es wird nicht unnütz sein, noch einen andern Beweis dieses Satzes anzufügen, der zu dem vorigen eine ähnliche Beziehung hat, wie der zweite Beweis (Artikel 109) des Satzes im Artikel 108 zum ersten (Artikel 108). Kundige werden dann leichter erkennen, dass sowohl jene wie diese beiden Beweise nicht so sehr verschieden sind, wie es vielleicht auf den ersten Blick erscheinen möchte.

I. Für einen beliebigen Primzahlmodul von der Form $4m+1$ finden sich unter den Zahlen $1, 2, 3, \ldots, 4m$, welche kleiner als der Modul sind, m Zahlen, welche einem Biquadrate congruent sein können, während die $3m$ übrigen dies nicht können.

Man könnte dies zwar leicht aus den Prinzipien des vorigen Abschnitts ableiten, doch ist der Beweis auch ohne diese nicht schwierig. Wir haben nämlich bewiesen, dass für einen solchen Modul -1 stets quadratischer

*) Kürzer wird der Beweis so geführt: Es ist $(a^{3n}-a^n)^2 = 2+(a^{4n}+1)(a^{2n}-2)$ und $(a^{3n}+a^n)^2 = -2+(a^{4n}+1)(a^{2n}+2)$. Mithin $\sqrt{2} \equiv \pm(a^{3n}-a^n)$ und $\sqrt{-2} \equiv \pm(a^{3n}+a^n) \pmod{8n+1}$.

Rest ist. Ist also $f^2 \equiv -1$, so werden offenbar, wenn z irgend eine durch den Modul nicht teilbare Zahl ist, die Biquadrate der vier Zahlen $+z$, $-z$, $+fz$, $-fz$ (die, wie man leicht sieht, einander incongruent sind) einander congruent sein. Ferner ist klar, dass das Biquadrat irgend einer Zahl, welche keiner von diesen vier congruent ist, den Biquadraten jener nicht congruent werden kann (denn sonst würde im Widerspruch mit Artikel 43 die Congruenz $x^4 \equiv z^4$, welche vom vierten Grade ist, mehr als vier Wurzeln haben). Hieraus folgert man leicht, dass sämtliche Zahlen $1, 2, 3, \ldots, 4m$ nur m incongruente Biquadrate erzeugen, denen unter denselben Zahlen m Zahlen congruent sind, während die übrigen keinem Biquadrate congruent sein können.

II. Nach einem Primzahlmodul von der Form $8n+1$ kann -1 einem Biquadrate congruent werden (-1 wird **biquadratischer** Rest dieser Primzahl sein).

Die Anzahl aller biquadratischen Reste, welche kleiner als $8n+1$ sind (die Null ausgeschlossen), ist nämlich gleich $2n$, d. h. gerade. Ferner zeigt man leicht, dass, wenn r biquadratischer Rest von $8n+1$ ist, auch der Wert des Ausdrucks $\frac{1}{r}$ (mod. $8n+1$) ein solcher Rest ist. Hiernach können sämtliche biquadratischen Reste in ähnlicher Weise in Klassen verteilt werden, wie wir dies im Artikel 109 mit den quadratischen Resten gethan haben. Ebenso schreitet auch der übrige Teil des Beweises in ganz derselben Weise fort wie dort.

III. Nun sei $g^4 \equiv -1$ und h der Wert des Ausdrucks $\frac{1}{g}$ (mod. $8n+1$). Dann wird (wegen $gh \equiv 1$):

$$(g \pm h)^2 = g^2 + h^2 \pm 2gh \equiv g^2 + h^2 \pm 2.$$

Nun ist aber $g^4 \equiv -1$, somit $-h^2 \equiv g^4 h^2 \equiv g^2$, also $g^2 + h^2 \equiv 0$ und $(g \pm h)^2 \equiv \pm 2$, d. h. sowohl $+2$ wie -2 ist quadratischer Rest von $8n+1$.

116.

Übrigens leitet man aus dem Vorhergehenden leicht die folgende **allgemeine Regel** her:

$+2$ ist Rest jeder Zahl, welche weder durch 4 noch durch irgend eine Primzahl von der Form $8n+3$ oder $8n+5$ teilbar ist, dagegen Nichtrest aller übrigen (z. B. aller Zahlen von den Formen $8n+3$ und $8n+5$, mögen dieselben Primzahlen oder zusammengesetzte Zahlen sein).

-2 ist Rest jeder Zahl, welche weder durch 4 noch durch irgend eine Primzahl von der Form $8n+5$ oder $8n+7$ teilbar ist, dagegen Nichrest aller übrigen.

Diese eleganten Sätze waren bereits dem scharfsinnigen Fermat bekannt, *Op. Mathem. p. 168*. Einen Beweis aber, in dessen Besitze er zu

sein behauptet, hat er nirgends mitgeteilt. Später ist ein solcher von Euler stets vergeblich gesucht worden; dagegen fand Lagrange zuerst einen strengen Beweis, *Nouv. Mém. de l'Ac. de Berlin 1775, p. 349, 351.* Dies scheint Euler noch nicht bekannt gewesen zu sein, als er seine in den *Opusc. Analyt. T. I, p. 259* aufbewahrte Abhandlung schrieb.

Reste + 3 und — 3.

117.

Wir gehen zu den Resten + 3 und — 3 über und beginnen mit dem letzteren.

Von Primzahlen, deren Rest — 3 ist, findet man aus der Tafel II die folgenden: 3, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97. Unter diesen kommt keine von der Form $6n+5$ vor. Dass es aber auch jenseits der Grenzen der Tafel keine Primzahlen von dieser Form, deren Rest — 3 ist, giebt, beweisen wir folgendermassen: Zunächst ist klar, dass jede zusammengesetzte Zahl von der Form $6n+5$ notwendig einen Primfactor von eben derselben Form enthält. Bis zu der Grenze also, bis zu welcher es keine Primzahlen von der Form $6n+5$ giebt, deren Rest — 3 ist, wird es auch keine solchen zusammengesetzten Zahlen geben. Wenn es aber jenseits der Grenzen unsrer Tafel solche Zahlen gäbe, so sei die kleinste von allen gleich t und es werde $-3 = a^2 - tu$ gesetzt. Dann wird, wenn man a gerade und kleiner als t annimmt, $u < t$ und — 3 Rest von u sein. Wenn aber a von der Form $6n \pm 2$ ist, so ist tu von der Form $6n+1$ und daher u von der Form $6n+5$. Dies ist aber absurd, da nach unsrer Annahme t die kleinste Zahl ist, für welche unser Inductionsschluss nicht gilt. Ist aber a von der Form $6n$, so wird tu von der Form $36n+3$ und daher $\frac{1}{3}tu$ von der Form $12n+1$, also $\frac{1}{3}u$ von der Form $6n+5$ sein. Offenbar aber ist — 3 Rest von $\frac{1}{3}u$ und $\frac{1}{3}u < t$. Dies ist aber absurd. Daher ist klar, dass — 3 von keiner Zahl von der Form $6n+5$ Rest sein kann.

Da jede Zahl von der Form $6n+5$ notwendig entweder unter der Form $12n+5$ oder unter der Form $12n+11$ enthalten ist und die erste wieder unter die Form $4n+1$, die letzte aber unter die Form $4n+3$ fällt, so hat man folgende **Sätze**:

I. Von jeder Primzahl von der Form $12n+5$ ist sowohl — 3 wie + 3 Nichtrest.

II. Von jeder Primzahl von der Form $12n+11$ ist — 3 Nichtrest, + 3 dagegen Rest.

118.

Als Zahlen, deren Rest + 3 ist, findet man aus der Tafel II die folgenden: 3, 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97, und unter diesen befindet sich keine Zahl von der Form $12n+5$ oder $12n+7$. Dass es aber

überhaupt keine Zahlen von den Formen $12n + 5$, $12n + 7$ giebt, deren Rest $+ 3$ ist, kann auf ganz dieselbe Weise bewiesen werden, wie in den Artikeln 112, 113, 117, weshalb wir uns hier der Mühe überheben. In Verbindung mit Artikel 111 erhalten wir daher folgende **Sätze**:

I. Von jeder Primzahl von der Form $12n + 5$ ist sowohl $+ 3$ wie $- 3$ Nichtrest (wie wir schon im vorigen Artikel gefunden haben).

II. Von jeder Primzahl von der Form $12n + 7$ ist $+ 3$ Nichtrest, $- 3$ dagegen Rest.

119.

Auf diesem Wege aber lässt sich nichts hinsichtlich der Zahlen von der Form $12n + 1$ finden, die demnach besondere Kunstgriffe erfordern. Auf inductivem Wege kann man zwar leicht folgern, dass $+ 3$ und $- 3$ Reste von allen Primzahlen dieser Form sind. Man braucht aber offenbar nur zu beweisen, dass $- 3$ von allen solchen Zahlen Rest ist, weil dann notwendig auch $+ 3$ Rest sein muss (Artikel 111). Wir werden jedoch allgemeiner beweisen, dass $- 3$ Rest einer jeden Primzahl von der Form $3n + 1$ ist.

Es sei p eine derartige Primzahl und a eine für den Modul p zum Exponenten 3 gehörige Zahl (dass es solche giebt, geht aus Artikel 54 hervor, weil 3 ein Teiler von $p - 1$ ist). Dann ist also $a^3 \equiv 1 \pmod{p}$, d. h. $a^3 - 1$ oder $(a^2 + a + 1)(a - 1)$ ist durch p teilbar. Offenbar kann aber nicht $a \equiv 1 \pmod{p}$ sein, da 1 zum Exponenten 1 gehört, mithin wird nicht $a - 1$, sondern vielmehr $a^2 + a + 1$, also auch $4a^2 + 4a + 4$ durch p teilbar sein, d. h. es ist $(2a + 1)^2 \equiv - 3 \pmod{p}$ oder $- 3$ ist Rest von p.

Übrigens ist klar, dass dieser Beweis (welcher von dem Vorhergehenden unabhängig ist) auch die Primzahlen von der Form $12n + 7$, die wir schon im vorigen Artikel abgethan haben, umfasst.

Man kann auch noch bemerken, dass diese Untersuchung nach Analogie der in den Artikeln 109, 115 angewandten Methode geführt werden kann, doch halten wir uns der Kürze wegen damit nicht auf.

120.

Aus dem Vorhergehenden ergeben sich leicht folgende **Sätze**: (Vgl. Artikel 102, 103, 105):

I. $- 3$ ist Rest aller Zahlen, welche weder durch 8 noch durch 9 noch durch irgend eine Primzahl von der Form $6n + 5$ teilbar sind, dagegen Nichtrest aller übrigen.

II. $+ 3$ ist Rest aller Zahlen, welche weder durch 4 noch durch 9 noch durch irgend eine Primzahl von der Form $12n + 5$ oder $12n + 7$ teilbar sind, dagegen Nichtrest aller übrigen.

Insbesondere möge man sich folgenden speciellen Fall merken.

$- 3$ ist Rest aller Primzahlen von der Form $3n + 1$, oder, was dasselbe ist, aller Primzahlen, welche Reste von 3 sind, Nicht-

rest dagegen aller Primzahlen von der Form $6n+5$ oder, mit Ausschluss von 2, aller Primzahlen von der Form $3n+2$, d. h. aller derer, die Nichtreste von 3 sind. Man erkennt leicht, dass hieraus alle übrigen Fälle von selbst folgen.

Die auf die Reste $+3$ und -3 bezüglichen Sätze sind schon Fermat bekannt gewesen, *Opera Wallisii, T. II. p. 857,* doch gab zuerst Euler die Beweise, *Comm. Nov. Petr. T. VIII p. 105 u. ff.* Um so mehr muss man sich wundern, dass die Beweise der auf die Reste $+2$ und -2 bezüglichen Sätze, die auf ganz ähnlichen Kunstgriffen beruhen, seinem Scharfsinn stets entgangen sind. Man vergleiche auch die Abhandlung von Lagrange, *Nouv. Mém. de l'Ac. de Berlin 1775 p. 352.*

Reste $+5$ und -5.

121.

Durch Induction findet man, dass $+5$ von keiner ungeraden Zahl von der Form $5n+2$ oder $5n+3$ Rest ist, d. h. von keiner ungeraden Zahl, welche Nichtrest von 5 ist. Dass aber diese Regel keine Ausnahme erleidet, wird so bewiesen: Es sei, wenn es eine giebt, die kleinste Zahl, welche von dieser Regel auszunehmen ist, gleich t, so dass dieselbe Nichtrest der Zahl 5 ist, während 5 Rest von t ist. Es sei ferner $a^2 = 5 + tu$, so dass a gerade und kleiner als t ist. Dann wird also u ungerade und kleiner als t, $+5$ aber Rest von u sein. Wenn nun a nicht durch 5 teilbar ist, so wird dasselbe von u gelten; offenbar aber ist tu Rest von 5, somit wird, da t Nichtrest von 5 ist, auch u Nichtrest von 5 sein. D. h. es giebt einen ungeraden Nichtrest der Zahl 5, dessen Rest $+5$ ist und der kleiner als t ist. Dies steht aber im Widerspruch mit unsrer Voraussetzung. Ist dagegen a durch 5 teilbar, so setze man $a = 5b$ und $u = 5v$, so wird $tv \equiv -1 \equiv 4$ (mod. 5), d. h. tv wird Rest der Zahl 5 sein. Im Übrigen schreitet der Beweis ebenso fort, wie im ersteren Falle.

122.

Von allen Primzahlen also, welche zu gleicher Zeit Nichtreste von 5 und von der Form $4n+1$ sind, d. h. von allen Primzahlen von der Form $20n+13$ oder $20n+17$, sind $+5$ und -5 Nichtreste; von allen Primzahlen von der Form $20n+3$ oder $20n+7$ dagegen ist $+5$ Nichtrest, -5 aber Rest.

Auf ganz analoge Weise kann man zeigen, dass -5 Nichtrest ist von allen Primzahlen von einer der Formen $20n+11$, $20n+13$, $20n+17$, $20n+19$, und hieraus folgt, wie man leicht sieht, dass $+5$ Rest ist von allen Primzahlen von der Form $20n+11$ oder $20n+19$, dagegen Nichtrest aller derer von der Form $20n+13$ oder $20n+17$. Und da jede Primzahl ausser 2 und 5 (von denen ± 5 Rest ist) in irgend einer der Formen $20n+1$, 3, 7, 9, 11, 13, 17, 19 enthalten ist, so kann man offenbar

bereits über alle ein Urteil fällen, ausser über diejenigen, welche von der Form $20n+1$ oder von der Form $20n+9$ sind.

123.

Durch Induction findet man leicht, dass $+5$ und -5 Reste aller Primzahlen von der Form $20n+1$ oder $20n+9$ sind. Wenn nun dies allgemein richtig wäre, so hätte man das elegante Gesetz, dass $+5$ Rest ist aller Primzahlen, welche Reste von 5 sind (denn diese sind in einer der beiden Formen $5n+1$ oder $5n+4$ oder in irgend einer der Formen $20n+1$, 9, 11, 19 enthalten und von der dritten und vierten der letztern ist jenes bereits bewiesen worden), Nichtrest aber von allen ungeraden Primzahlen, welche Nichtreste von 5 sind, wie wir schon oben bewiesen haben. Es ist aber klar, dass dieser Satz genügt, um zu entscheiden, ob $+5$ (und somit auch -5, wenn man dies als Product aus $+5$ und -1 betrachtet) Rest oder Nichtrest irgend einer gegebenen Zahl ist. Schliesslich möge man die Analogie dieses Satzes mit demjenigen, welchen wir im Artikel 120 hinsichtlich des Restes -3 angeführt haben, bemerken.

Die Bestätigung jenes Inductionsschlusses ist jedoch nicht allzu leicht. Ist eine Primzahl von der Form $20n+1$ oder allgemeiner von der Form $5n+1$ gegeben, so kann man die Sache in ähnlicher Weise erledigen, wie in den Artikeln 114, 119. Ist nämlich a irgend eine für den Modul $5n+1$ zum Exponenten 5 gehörige Zahl (dass es dergleichen giebt, geht aus dem vorigen Abschnitt hervor), so ist $a^5 \equiv 1$ oder $(a-1)(a^4+a^3+a^2+a+1) \equiv 0$ (mod. $5n+1$). Da aber nicht $a \equiv 1$ und somit auch nicht $a-1 \equiv 0$ sein kann, so wird notwendig $a^4+a^3+a^2+a+1 \equiv 0$ sein. Daher ist auch $4(a^4+a^3+a^2+a+1) = (2a^2+a+2)^2 - 5a^2 \equiv 0$, d. h. $5a^2$ ist Rest von $5n+1$, und somit ist auch 5 Rest von $5n+1$, weil a^2 ein durch $5n+1$ nicht teilbarer Rest ist (denn a ist durch $5n+1$ nicht teilbar wegen $a^5 \equiv 1$).

Der Fall aber, wo eine Primzahl von der Form $5n+4$ gegeben ist, erfordert tieferliegende Hülfsmittel. Da jedoch die Sätze, mit deren Hülfe die Sache erledigt wird, im folgenden allgemeiner werden behandelt werden, so wollen wir sie hier nur kurz berühren.

I. Wenn p eine Primzahl und b ein gegebener quadratischer Nichtrest von p ist, so ist der Wert des Ausdrucks

$$(A) \qquad \frac{(x+\sqrt{b})^{p+1}-(x-\sqrt{b})^{p+1}}{\sqrt{b}}$$

(aus welchem, wie man leicht sieht, die Irrationalität nach der Entwicklung herausfällt) durch p teilbar, welche Zahl man auch für x nehmen möge. Aus dem blossen Anblick der Coefficienten, welche aus der Entwicklung von A erhalten werden, geht nämlich hervor, dass alle Glieder vom zweiten bis zum vorletzten einschliesslich durch p teilbar sind und dass somit

$A \equiv 2(p+1)(x^p + xb^{\frac{p-1}{2}})$ (mod. p) ist. Da aber b Nichtrest von p ist, so ist $b^{\frac{p-1}{2}} \equiv -1$ (mod. p) (Artikel 106); x^p ist aber stets $\equiv x$ (nach vorigem Abschnitt); somit $A \equiv 0$.

II. In der Congruenz $A \equiv 0$ (mod. p) hat die Unbestimmte x p Dimensionen und sämtliche Zahlen 0, 1, 2, ..., $p-1$ sind Wurzeln derselben. Nimmt man nun an, dass e ein Teiler von $p+1$ sei, so wird der Ausdruck

$$\frac{(x+\sqrt{b})^e - (x-\sqrt{b})^e}{\sqrt{b}}$$

(den wir mit B bezeichnen) nach der Entwicklung von der Irrationalität frei werden, die Unbestimmte x wird in ihm $e-1$ Dimensionen besitzen, und es wird, wie aus den ersten Elementen der Analysis bekannt ist, A durch B (unbestimmt) teilbar sein. Nun behaupte ich, dass es $e-1$ Werte von x giebt, welche, in B eingesetzt, B durch p teilbar machen. Setzt man nämlich $A \equiv BC$, so wird x in C $p-e+1$ Dimensionen und daher die Congruenz $C \equiv 0$ (mod. p) nicht mehr als $p-e+1$ Wurzeln besitzen. Hieraus folgt leicht, dass alle übrigen $e-1$ Zahlen aus der Reihe 0, 1, 2, 3, ..., $p-1$ Wurzeln der Congruenz $B \equiv 0$ sind.

III. Man nehme nun an, dass p von der Form $5n+4$, $e=5$, b Nichtrest von p und die Zahl a derart bestimmt sei, dass der Ausdruck

$$\frac{(a+\sqrt{b})^5 - (a-\sqrt{b})^5}{\sqrt{b}}$$

durch p teilbar ist. Jener Ausdruck aber ist:

$$= 10a^4 + 20a^2b + 2b^2 = 2\left((b+5a^2)^2 - 20a^4\right);$$

somit wird auch $(b+5a^2)^2 - 20a^4$ durch p teilbar, d. h. $20a^4$ ist Rest von p. Da aber $4a^4$ ein durch p nicht teilbarer Rest ist (denn man sieht leicht, dass a durch p nicht teilbar ist), so wird auch 5 Rest von p sein, was bewiesen werden sollte.

Hieraus geht hervor, dass der im Anfang dieses Artikels angegebene Satz allgemein richtig ist.

Wir bemerken noch, dass man die Beweise für beide Fälle Lagrange verdankt, *Mém. de l'Ac. de Berlin 1775 p. 352 u. ff.*

Ueber ± 7.

124.

Durch ein ähnliches Verfahren beweist man,

dass -7 Nichtrest ist von jeder Zahl, die Nichtrest von 7 ist.

Durch Induction aber kann man schliessen,
dass -7 Rest ist von jeder Primzahl, die Rest von 7 ist.

Dies ist jedoch bisher von Niemand streng bewiesen worden. Zwar ist für diejenigen Reste von 7, welche von der Form $4n-1$ sind, der Beweis leicht. Denn auf dem aus dem Vorhergehenden genugsam bekannten Wege kann man zeigen, dass $+7$ stets Nichtrest und somit -7 Rest derartiger Primzahlen ist. Aber hiermit ist wenig gewonnen, da man die übrigen Fälle nicht nach dieser Methode behandeln kann. Nur einen Fall können wir noch auf ähnliche Weise wie in Artikel 119 und 123 erledigen. Ist nämlich p eine Primzahl von der Form $7n+1$ und a für den Modul p eine zum Exponenten 7 gehörige Zahl, so sieht man leicht, dass der Ausdruck

$$\frac{4(a^7-1)}{a-1} = (2a^3+a^2-a-2)^2+7(a^2+a)^2$$

durch p teilbar und somit $-7(a^2+a)^2$ Rest von p ist. Es ist aber $(a^2+a)^2$ als Quadrat Rest von p und überdies nicht teilbar durch p; denn da a der Annahme nach zum Exponenten 7 gehört, so kann es weder $\equiv 0$ noch $\equiv -1 \pmod{p}$ sein, d. h. es ist weder a noch $a+1$ durch p teilbar und daher auch nicht das Quadrat $(a+1)^2a^2$. Somit ist offenbar auch 7 Rest von p, was bewiesen werden sollte. — Für die Primzahlen von der Form $7n+2$ oder $7n+4$ aber schlagen alle bisher angegebenen Methoden fehl. Übrigens ist auch dieser Beweis zuerst von Lagrange gefunden worden, a. a. O. — Unten im Abschnitt VII werden wir allgemein beweisen, dass der Ausdruck $\frac{4(x^p-1)}{x-1}$ immer auf die Form $X^2 \mp pY^2$ (wo das obere Zeichen zu nehmen ist, wenn p eine Primzahl von der Form $4n+1$, das untere, wenn es eine solche von der Form $4n+3$ ist) gebracht werden kann, wo X und Y rationale von Brüchen freie Functionen von x sind. Diese Zerlegung hat Lagrange über den Fall $p=7$ hinaus nicht ausgeführt. Vgl. a. a. O. S. 352.

Vorbereitung auf die allgemeine Untersuchung.

125.

Da somit die vorher angewandten Methoden zur Führung der allgemeinen Beweise nicht ausreichen, ist es Zeit, eine andere von diesem Mangel freie Methode darzulegen. Wir beginnen mit einem Satze, den zu beweisen unsern Bemühungen lange nicht gelingen wollte, obwohl die Richtigkeit desselben auf den ersten Blick so offenbar zu sein scheint, dass manche nicht einmal die Notwendigkeit eines Beweises anerkannt haben. Es ist der folgende: Jede beliebige Zahl, mit Ausnahme der positiv genommenen Quadrate, ist Nichtrest irgend welcher Primzahlen. Da wir uns aber dieses Satzes nur als eines Hülfssatzes zum

Beweise anderer bedienen werden, so entwickeln wir hier nur diejenigen Fälle, deren wir zu diesem Zweck bedürfen. Die Richtigkeit der übrigen Fälle wird später von selbst sich ergeben. Wir zeigen daher, dass jede Primzahl von der Form $4n+1$, mag sie positiv oder negativ genommen werden*), Nichtrest irgendwelcher Primzahlen ist, und zwar (falls sie >5 ist) von solchen, die kleiner als sie selbst sind.

Zunächst sei, wenn eine Primzahl p von der Form $4n+1$ (und >17; jedoch ist -13 Nichtrest von 3, -17 Nichtrest von 5), die negativ genommen werden soll, gegeben ist, $2a$ die erste gerade Zahl, welche grösser ist als $\sqrt{p}$; dann sieht man leicht, dass stets $4a^2<2p$ oder $4a^2-p<p$ ist. Nun ist aber $4a^2-p$ von der Form $4n+3$, während $+p$ quadratischer Rest von $4a^2-p$ ist $\left(\text{da } p\equiv 4a^2 \pmod{4a^2-p}\right)$. Wenn daher $4a^2-p$ eine Primzahl ist, so wird $-p$ Nichtrest von ihr sein; wenn nicht, so muss notwendig irgend ein Factor von $4a^2-p$ von der Form $4n+3$ sein, und da $+p$ auch von diesem Rest sein muss, so wird $-p$ Nichtrest desselben sein.

Bezüglich der Primzahlen, welche positiv genommen werden sollen, unterscheiden wir zwei Fälle. Zuerst sei p eine Primzahl von der Form $8n+5$. Ist a eine beliebige positive Zahl $<\sqrt{\frac{1}{2}p}$, so ist $8n+5-2a^2$ eine positive Zahl von der Form $8n+5$ oder $8n+3$ (je nachdem a gerade oder ungerade ist) und daher notwendig durch irgend eine Primzahl von der Form $8n+3$ oder $8n+5$ teilbar, da das Product aus beliebig vielen Zahlen von der Form $8n+1$ und $8n+7$ weder die Form $8n+3$ noch die Form $8n+5$ haben kann. Ist dieselbe gleich q, so wird $8n+5\equiv 2a^2 \pmod{q}$. Nun ist aber 2 Nichtrest von q (Artikel 112), somit auch $2a^2$**) und $8n+5$.

126.

Dass aber jede Primzahl von der Form $8n+1$, positiv genommen, stets Nichtrest irgend einer Primzahl ist, welche kleiner als sie selbst ist, lässt sich nicht durch so auf der Hand liegende Hülfsmittel beweisen. Da jedoch diese Wahrheit von der grössten Wichtigkeit ist, können wir einen strengen Beweis, obwohl derselbe ziemlich weitläufig ist, nicht übergehen. Wir schicken voraus den folgenden

Hülfssatz. Wenn man zwei Reihen von Zahlen

(I) $A, B, C, \ldots.$
(II) $A', B', C', \ldots.$

(ob die Anzahl der Glieder in beiden dieselbe ist oder nicht, darauf kommt es nicht an) von solcher Beschaffenheit hat, dass, wenn p irgend eine Primzahl oder eine Potenz einer Primzahl, welche in irgend

*) Dass $+1$ ausgenommen werden muss, ist von selbst klar.

**) Artikel 98. Offenbar ist nämlich a^2 ein durch q nicht teilbarer Rest von q, denn sonst würde auch die Primzahl p durch q teilbar sein, was absurd ist.

einem Gliede (oder auch in mehreren Gliedern) der zweiten Reihe aufgeht, bezeichnet, mindestens ebenso viele Glieder in der ersten Reihe durch p teilbar sind, wie in der zweiten, so behaupte ich, ist das Product aus allen Zahlen (I) teilbar durch das Product aus allen Zahlen (II).

Beispiel. Besteht (I) aus den Zahlen 12, 18, 45, (II) aus den Zahlen 3, 4, 5, 6, 9, so sind durch 2, 4, 3, 9, 5 in (I) respective 2, 1, 3, 2, 1 Glieder, in (II) respective 2, 1, 3, 1, 1 Glieder teilbar. Das Product aus allen Gliedern von (I), welches gleich 9720 ist, ist aber teilbar durch das Product aller Glieder von (II), nämlich durch 3240.

Beweis. Ist das Product aus allen Gliedern (I) gleich Q, das Product aus allen Gliedern (II) gleich Q', so ist offenbar jede Primzahl, welche Teiler von Q' ist, auch Teiler von Q. Wir werden nun zeigen, dass jeder Primfactor von Q' in Q mindestens ebenso viel Dimensionen besitzt, wie in Q'. Es sei p ein solcher Teiler und man nehme an, dass in der Reihe (I) a Glieder durch p, b Glieder durch p^2, c Glieder durch p^3, u. s. w. teilbar seien und dass die Buchstaben a' b' c', ... für die Reihe (II) die analoge Bedeutung haben, so sieht man leicht, dass p in Q $a+b+c+\cdots$, in Q' aber $a'+b'+c'+\cdots$ Dimensionen hat. Nun ist aber nach Voraussetzung a' sicher nicht grösser als a, b' nicht grösser als b, u. s. w., somit sicher $a'+b'+c'+\cdots$ nicht $> a+b+c+\cdots$ — Da mithin keine Primzahl in Q' mehr Dimensionen haben kann, als in Q, so ist Q durch Q' teilbar (Artikel 17).

127.

Hülfssatz. In der Progression 1, 2, 3, 4, ..., n kann es nicht mehr durch irgend eine Zahl h teilbare Glieder geben, als in der aus ebensovielen Gliedern bestehenden Reihe a, $a+1$, $a+2$, ..., $a+n-1$.

Man sieht nämlich ohne Schwierigkeit, dass, wenn n ein Vielfaches von h ist, in jeder der beiden Progressionen $\frac{n}{h}$ Glieder durch h teilbar sind. Ist jenes nicht der Fall, so setze man $n = eh + f$, so dass $f < h$ ist; dann werden in der ersten Reihe e Glieder, in der zweiten aber entweder ebenso viel oder $e+1$ Glieder durch h teilbar sein.

Hieraus folgt als Zusatz der aus der Lehre von den figurierten Zahlen bekannte, aber bisher, wenn wir nicht irren, noch von Niemand direct bewiesene Satz, dass

$$\frac{a\,(a+1)\,(a+2)\cdots(a+n-1)}{1\cdot 2\cdot 3\cdots n}$$

immer eine ganze Zahl ist.

Schliesslich hätte man diesen Hülfssatz allgemeiner so aussprechen können:

In der Progression a, $a+1$, $a+2$, ..., $a+n-1$ giebt es mindestens ebenso viele einer gegebenen Zahl r nach dem Modul h congruente Glieder, als es in der Reihe 1, 2, 3, ..., n durch h teilbare Glieder giebt.

128.

Satz. Ist a irgend eine Zahl von der Form $8n+1$, p irgend eine zu a prime Zahl, deren Rest $+a$ ist, schliesslich m eine beliebige Zahl, so behaupte ich, dass es in der Progression

$$a, \tfrac{1}{2}(a-1), 2(a-4), \tfrac{1}{2}(a-9), 2(a-16), \ldots, 2(a-m^2) \text{ oder } \tfrac{1}{2}(a-m^2),$$

je nachdem m gerade oder ungerade ist, mindestens ebenso viele durch p teilbare Glieder giebt als in der folgenden:

$$1, 2, 3, \ldots, 2m+1.$$

Die erste Progession bezeichnen wir mit (I), die zweite mit (II).

Beweis. I. Ist $p=2$, so werden in (I) alle Glieder mit Ausnahme des ersten d. h. m Glieder durch p teilbar sein; ebensoviele auch in (II).

II. Ist p eine ungerade Zahl oder das Doppelte oder Vielfache einer ungeraden Zahl und $a \equiv r^2 \pmod{p}$, so werden in der Progression $-m$, $-(m-1)$, $-(m-2)$, ..., $+m$ (welche in der Anzahl der Glieder mit (II) übereinstimmt und mit (III) bezeichnet werden möge) mindestens ebenso viele der Zahl r nach dem Modul p congruente Glieder enthalten sein, als es in der Reihe (II) durch p teilbare Glieder giebt (nach vorigem Artikel). Unter jenen können sich aber nicht zwei, die sich nur durch das Vorzeichen, nicht aber durch die Grösse unterscheiden, vorfinden.*) Schliesslich wird jedes derselben in der Reihe (I) ein entsprechendes haben, welches durch p teilbar ist. Wenn nämlich $\pm b$ irgend ein Glied der Reihe (III) ist, welches r nach p congruent ist, so wird $a-b^2$ durch p teilbar sein. Ist nun b gerade, so ist das Glied $2(a-b^2)$ der Reihe (I) durch p teilbar. Ist aber b ungerade, so ist das Glied $\frac{1}{2}(a-b^2)$ durch p teilbar; denn offenbar ist $\frac{a-b^2}{p}$ eine gerade ganze Zahl, da $a-b^2$ durch 8, p aber höchstens durch 4 teilbar ist (denn a ist nach Voraussetzung von der Form $8n+1$, b^2 aber ist aus dem Grunde, weil es das Quadrat einer ungeraden Zahl ist, von derselben Form, somit ist ihre Differenz von der Form $8n$). Hieraus schliesst man endlich, dass in der Reihe (I) ebenso viele Glieder durch p teilbar sind, als es in der Reihe (III) der Zahl r nach dem Modul p congruente Glieder giebt, d. h. ebenso viel oder mehr Glieder, als in (II) durch p teilbar sind.

*) Wäre nämlich $r \equiv -f \equiv +f \pmod{p}$, so würde $2f$ durch p teilbar und somit auch (wegen $f^2 \equiv a \pmod{p}$) $2a$ durch p teilbar sein. Dies ist aber nur möglich, wenn $p=2$ ist, da nach Voraussetzung a prim zu p ist. Über den Fall $p=2$ haben wir aber bereits besonders gehandelt.

III. Es sei p von der Form $8n$ und $a \equiv r^2$ (mod. $2p$). Denn man sieht leicht, dass a, da es nach Voraussetzung Rest von p ist, auch Rest von $2p$ sein wird. Dann wird es in der Reihe (III) mindestens ebenso viele r nach dem Modul p congruente Glieder geben, als in (II) durch p teilbar sind, und jene werden sämtlich der Grösse nach verschieden sein. Aber einem jeden von ihnen wird in der Reihe (I) irgend ein durch p teilbares Glied entsprechen. Denn wenn $+b$ oder $-b \equiv r$ (mod. p) ist, so wird $b^2 \equiv r^2$ (mod. $2p$)*) und daher ist das Glied $\frac{1}{2}(a-b)^2$ durch p teilbar. Somit giebt es in (I) mindestens ebenso viele durch p teilbare Glieder wie in (II).

129.

Satz. Ist a eine Primzahl von der Form $8n+1$, so giebt es unterhalb $2\sqrt{a}+1$ notwendig irgend eine Primzahl, von welcher a Nichtrest ist.

Beweis. Es sei, wenn dies möglich ist, a Rest aller Primzahlen, welche kleiner als $2\sqrt{a}+1$ sind. Dann sieht man leicht, dass a auch von allen zusammengesetzten Zahlen, die kleiner als $2\sqrt{a}+1$ sind, Rest sein wird (man vergleiche die Regeln, nach denen man entscheiden kann, ob eine gegebene Zahl von einer zusammengesetzten Zahl Rest ist oder nicht, Artikel 105). Es sei die grösste ganze Zahl unterhalb $\sqrt{a}$ gleich m, so werden in der Reihe

(I) $a,\ \frac{1}{2}(a-1),\ 2(a-4),\ \frac{1}{2}(a-9),\ \ldots,\ 2(a-m^2)$ oder $\frac{1}{2}(a-m^2)$

ebenso viele oder mehr durch eine unterhalb $2\sqrt{a}+1$ liegende Zahl teilbare Glieder vorkommen wie in der folgenden:

(II) $1,\ 2,\ 3,\ 4,\ \ldots,\ 2m+1$ (nach vorigem Artikel).

Hieraus folgt aber, dass das Product aus allen Gliedern der Reihe (I) durch das Product aus allen Gliedern der Reihe (II) teilbar ist (Artikel 126). Jenes ist aber entweder gleich $a(a-1)(a-4)\ldots(a-m^2)$ oder gleich der Hälfte dieses Products (je nachdem m gerade oder ungerade ist). Daher ist das Product $a(a-1)(a-4)\ldots(a-m^2)$ sicher durch das Product aller Glieder (II) und, da alle diese Glieder prim zu a sind, auch jenes Product nach Weglassung des Factors a teilbar. Das Product aus allen Gliedern (II) kann aber auch folgendermassen dargestellt werden:

$$(m+1)\,[(m+1)^2-1]\,[(m+1)^2-4]\cdots[(m+1)^2-m^2].$$

Somit wird

$$\frac{1}{m+1}\cdot\frac{a-1}{(m+1)^2-1}\cdot\frac{a-4}{(m+1)^2-4}\cdots\cdots\frac{a-m^2}{(m+1)^2-m^2}$$

*) Es ist nämlich $b^2-r^2=(b-r)(b+r)$ aus zwei Factoren zusammengesetzt, von denen der eine durch p (nach Voraussetzung), der andere (weil sowohl b als r ungerade ist) durch 2 teilbar ist; somit ist b^2-r^2 durch $2p$ teilbar.

eine ganze Zahl sein, obwohl es ein Product aus Brüchen ist, die kleiner als 1 sind; denn da $\sqrt{a}$ notwendig irrational sein muss, so ist $m+1>\sqrt{a}$ und daher $(m+1)^2>a$. Hieraus folgt schliesslich, dass unsere Annahme nicht stattfinden kann.

Weil nun a sicher >9 ist, so wird $2\sqrt{a}+1<a$, und somit giebt es unterhalb a irgend eine Primzahl, von welcher a Nichtrest ist.

Durch Induction wird ein allgemeiner (fundamentaler) Satz begründet und daraus werden Schlüsse gezogen.

130.

Nachdem wir streng bewiesen haben, dass jede Primzahl von der Form $4n+1$, sowohl positiv wie negativ genommen, Nichtrest irgend einer Primzahl ist, die kleiner als sie selbst ist, gehen wir sogleich zur genaueren und allgemeineren Vergleichung der Primzahlen, insofern die eine Rest oder Nichtrest einer andern ist, über.

Oben haben wir in aller Strenge bewiesen, dass -3 und $+5$ Reste oder Nichtreste aller Primzahlen sind, welche respective Reste oder Nichtreste von 3 oder 5 sind.

Durch eine mit den folgenden Zahlen angestellte Induction findet man, dass -7, -11, $+13$, $+17$, -19, -23, $+29$, -31, $+37$, $+41$, -43, -47, $+53$, -59 u. s. w. Reste oder Nichtreste aller Primzahlen sind, welche, positiv genommen, respective von jenen Primzahlen Reste oder Nichtreste sind. Diese Induction kann leicht mittelst der Tafel II durchgeführt werden.

Bei nur einiger Aufmerksamkeit wird jedermann bemerken, dass von diesen Primzahlen diejenigen, welche von der Form $4n+1$ sind, mit positivem, diejenigen aber, welche von der Form $4n+3$ sind, mit negativem Vorzeichen behaftet sind.

131.

Wir werden bald beweisen, dass das, was wir hier durch Induction gefunden haben, allgemein richtig ist. Bevor wir uns aber dieser Mühe unterziehen, wird es nötig sein, alles, was aus jenem Satze folgt, sofern er als richtig angenommen wird, anzugeben. Den **Satz** selbst sprechen wir folgendermassen aus:

Ist p eine Primzahl von der Form $4n+1$, so wird $+p$, ist dagegen p eine solche von der Form $4n+3$, so wird $-p$ Rest oder Nichtrest jeder Primzahl sein, welche, positiv genommen, Rest oder Nichtrest von p ist.

Da fast alles, was sich über die quadratischen Reste sagen lässt, auf diesem Satze beruht, so wird die Bezeichnung „**Fundamentalsatz**“, die wir im Folgenden gebrauchen werden, für denselben nicht unpassend sein.

Um unsere Schlüsse so kurz wie möglich darstellen zu können, werden wir mit $a, a', a'', \ldots$ Primzahlen von der Form $4n+1$, mit $b, b', b'', \ldots$

Primzahlen von der Form $4n+3$, ferner mit $A, A', A'', \ldots$ beliebige Zahlen von der Form $4n+1$ und mit $B, B', B'', \ldots$ beliebige Zahlen von der Form $4n+3$ bezeichnen. Schliesslich soll der zwischen zwei Grössen gesetzte Buchstabe R andeuten, dass der erste Rest des folgenden ist, und der Buchstabe N soll die entgegengesetzte Bedeutung haben. Z. B. bedeutet $+5R11$, $\pm 2N5$, dass $+5$ Rest von 11, $+2$ oder -2 Nichtrest von 5 ist. Hält man nun den Fundamentalsatz mit den Sätzen des Artikel 111 zusammen, so leitet man leicht folgende Sätze ab:

	Ist	so ist
1.	$\pm aRa'$	$\pm a'Ra$
2.	$\pm aNa'$	$\pm a'Na$
3.	$\left.\begin{matrix}+aRb\\-aNb\end{matrix}\right\}$	$\pm bRa$
4.	$\left.\begin{matrix}+aNb\\-aRb\end{matrix}\right\}$	$\pm bNa$
5.	$\pm bRa$	$\left\{\begin{matrix}+aRb\\-aNb\end{matrix}\right.$
6.	$\pm bNa$	$\left\{\begin{matrix}+aNb\\-aRb\end{matrix}\right.$
7.	$\left.\begin{matrix}+bRb'\\-bNb'\end{matrix}\right\}$	$\left\{\begin{matrix}+b'Nb\\-b'Rb\end{matrix}\right.$
8.	$\left.\begin{matrix}+bNb'\\-bRb'\end{matrix}\right\}$	$\left\{\begin{matrix}+b'Rb\\-b'Nb\end{matrix}\right.$

132.

Hierin sind alle Fälle, welche bei der Vergleichung zweier Primzahlen vorkommen können, enthalten; das Folgende bezieht sich auf beliebige Zahlen, doch liegen die Beweise dafür nicht so auf der Hand.

	Ist	so ist
9.	$\pm aRA$	$\pm ARa$
10.	$\pm bRA$	$\left\{\begin{matrix}+ARb\\-ANb\end{matrix}\right.$
11.	$+aRB$	$\pm BRa$
12.	$-aRB$	$\pm BNa$
13.	$+bRB$	$\left\{\begin{matrix}-BRb\\+BNb\end{matrix}\right.$
14.	$-bRB$	$\left\{\begin{matrix}+BRb\\-BNb\end{matrix}\right.$

Da die Beweise aller dieser Sätze aus denselben Prinzipien abzuleiten sind, wird es nicht nötig sein, alle ausführlich anzugeben; der Beweis des

Satzes 9, den wir anführen, kann als Beispiel dienen. Vor allem aber möge bemerkt werden, dass jede Zahl von der Form $4n + 1$ entweder gar keinen Factor von der Form $4n + 3$ hat oder zwei oder vier u. s. w., d. h. dass die Anzahl derartiger Factoren (unter denen auch gleiche sich befinden können) stets gerade ist, dass dagegen jede Zahl von der Form $4n + 3$ stets eine ungerade Anzahl Factoren von der Form $4n + 3$ (d. h. entweder einen oder drei oder fünf u. s. w.) enthält. Die Anzahl der Factoren von der Form $4n + 1$ bleibt unbestimmt.

Der Satz 9 wird folgendermassen bewiesen: Es sei A das Product aus den Primfactoren $a', a'', a''', \ldots, b, b', b'', \ldots$, wo die Anzahl der Factoren $b, b', b'', \ldots$ gerade ist (doch können auch gar keine solche vorhanden sein, was auf dasselbe hinauskommt). Wenn nun a Rest von A ist, so wird es auch Rest von allen Factoren $a', a'', a''', \ldots, b, b', b'', \ldots$ sein, somit sind nach den Sätzen 1 und 3 des vorhergehenden Artikels diese einzelnen Factoren und daher auch ihr Product A Reste von a. Dasselbe muss aber auch $-A$ sein. — Wenn aber $-a$ von A und daher auch von den einzelnen Factoren $a', a'', \ldots, b, b', \ldots$ Rest ist, so werden die einzelnen Factoren $a', a'', \ldots$ Reste von a, die Factoren $b, b', \ldots$ aber Nichtreste sein. Da jedoch die Anzahl der letzteren gerade ist, so ist das Product aus allen d. h. A Rest von a und somit auch $-A$.

133.

Wir stellen die Untersuchung noch allgemeiner an. Wir betrachten zwei beliebige zu einander prime ungerade Zahlen P und Q, die mit irgendwelchen Vorzeichen behaftet sind. Man denke sich P ohne Rücksicht auf sein Vorzeichen in seine Primfactoren zerlegt und bezeichne mit p, wie viele unter diesen sich finden, von denen Q Nichtrest ist. Kommt aber irgend eine Primzahl, von welcher Q Nichtrest ist, mehrere Male unter den Factoren von p vor, so ist es auch mehrere Male zu zählen. Analog sei q die Anzahl der Primfactoren von Q, von denen P Nichtrest ist. Dann werden die Zahlen p und q in einer gewissen Beziehung zu einander stehen, die von der Natur der Zahlen P, Q abhängt. Wenn nämlich die eine der Zahlen p, q gerade oder ungerade ist, wird die Form der Zahlen P, Q zeigen, ob die andere gerade oder ungerade ist. Diese Beziehung ist in der folgenden Tafel dargestellt.

Die Zahlen p, q werden gleichzeitig gerade oder ungerade sein, wenn die Zahlen P, Q die Formen haben:

1.	$+A$,	$+A'$
2.	$+A$,	$-A'$
3.	$+A$,	$+B$
4.	$+A$,	$-B$
5.	$-A$,	$-A'$
6.	$+B$,	$-B'$.

Dagegen wird von den Zahlen p, q die eine gerade, die andere ungerade sein, wenn die Zahlen P, Q die Formen haben:

7.	$-A$,	$+B$
8.	$-A$,	$-B$
9.	$+B$,	$+B'$
10.	$-B$,	$-B'$.*)

Beispiel. Die gegebenen Zahlen seien -55 und $+1197$, die zum vierten Fall gehören. Es ist aber 1197 Nichtrest eines einzigen Primfactors von 55, nämlich von der Zahl 5, -55 aber Nichtrest dreier Primfactoren von 1197, nämlich von den Zahlen 3, 3, 19.

Wenn P und Q Primzahlen bezeichnen, so gehen diese Sätze in diejenigen über, die wir im Artikel 131 angeführt haben. Hier können nämlich p und q nicht grösser werden als 1; wird daher p als gerade vorausgesetzt, so muss es notwendig $=0$ sein, d. h. Q ist Rest von P; ist aber p ungerade, so ist Q Nichtrest von P. Und umgekehrt. Schreibt man also hier a, b an Stelle von A, B, so folgt aus 8), dass, wenn $-a$ Rest oder Nichtrest von b ist, $-b$ Nichtrest oder Rest von a ist, was mit 3) und 4) des Artikels 131 übereinstimmt.

Allgemein aber ist klar, dass Q nur Rest von P sein kann, wenn $p=0$ ist; ist also p ungerade, so ist Q sicher Nichtrest von P.

Hieraus können auch die Sätze des vorhergehenden Artikels ohne Schwierigkeit abgeleitet werden.

Übrigens wird bald klar werden, dass diese allgemeine Darstellung mehr ist als eine unfruchtbare Spekulation, da der vollständige Beweis des Fundamentalsatzes kaum ohne dieselbe geführt werden kann.

134.

Wir gehen nun zur Ableitung dieser Sätze.

I. Man denke sich, wie vorher, P in seine Primfactoren mit Weglassung der Vorzeichen zerlegt und löse ferner auch Q auf irgendwelche Weise in Factoren auf, doch so, dass das Vorzeichen von Q in Rücksicht gezogen wird. Man combiniere darauf jeden einzelnen von jenen mit jedem einzelnen von diesen. Wenn dann s die Anzahl aller Combinationen bezeichnet, in welchen ein Factor von Q Nichtrest ist eines Factors von P, so werden p und s entweder gleichzeitig gerade oder gleichzeitig ungerade sein. Denn sind f, f', f'', ... die Primfactoren von P, und giebt es unter den Factoren, in welche Q aufgelöst ist, m, welche Nichtreste von f sind, m' Nichtreste von f', m'' Nichtreste von f'' u. s. w., so wird man leicht sehen, dass

$$s = m + m' + m'' + \cdots$$

*) Ist $l=1$, wenn beide Zahlen P, $Q \equiv 3 \pmod{4}$ sind, sonst $l=0$,
$m=1$, wenn beide Zahlen P, Q negativ sind, sonst $m=0$,
so hängt jene Beziehung von $l+m$ ab.

ist, dass aber p ausdrückt, wie viele unter den Zahlen m, m', m'', ... ungerade sind. Hieraus geht von selbst hervor, dass s gerade sein wird, wenn p gerade, dagegen ungerade, wenn p ungerade ist.

II. Dies gilt allgemein, auf welche Weise auch Q in Factoren zerlegt sein möge. Gehen wir jetzt zu speciellen Fällen über und betrachten wir zuerst die Fälle, wo die eine der Zahlen, P, positiv, die andere, Q, aber entweder von der Form $+A$ oder von der Form $-B$ ist. Man zerlege P und Q in ihre Primfactoren, erteile den einzelnen Factoren von P das positive Vorzeichen, den einzelnen Factoren von Q aber das positive oder negative Vorzeichen, je nachdem sie von der Form a oder b sind; dann wird offenbar Q entweder von der Form $+A$ oder von der Form $-B$ werden, wie erforderlich ist. Man combiniere die einzelnen Factoren von P mit den einzelnen Factoren von Q und bezeichne, wie vorher, mit s die Anzahl der Combinationen, in denen ein Factor von Q Nichtrest ist eines Factors von P, und analog mit t die Anzahl der Combinationen, in denen ein Factor von P Nichtrest ist eines Factors von Q. Dann folgt aus dem Fundamentalsatze, dass jene Combinationen identisch sind mit diesen und daher $s=t$ ist. Schliesslich folgt aus dem soeben Bewiesenen, dass $p\equiv s$ (mod. 2), $q\equiv t$ (mod. 2) ist, und somit wird $p\equiv q$ (mod. 2).

Man erhält somit die Sätze 1), 3), 4) und 6) des Artikels 133.

Die übrigen Sätze können auf ähnlichem Wege direct abgeleitet werden, doch bedürfen sie einer neuen Betrachtung. Leichter aber leitet man sie aus dem Vorhergehenden auf folgende Weise her.

III. Es bezeichnen wiederum P und Q irgendwelche zu einander prime ungerade Zahlen, p und q die Anzahl der Primfactoren von P, Q, von denen respective Q oder P Nichtrest ist. Endlich sei p' die Anzahl der Primfactoren von P, von denen $-Q$ Nichtrest ist (ist Q an sich negativ, so wird offenbar $-Q$ eine positive Zahl bezeichnen). Man teile nun alle Primfactoren von P in vier Klassen und zwar

1. in Factoren von der Form a, deren Rest Q ist,
2. in Factoren von der Form b, von denen Q Rest ist. Die Anzahl dieser sei gleich χ,
3. in Factoren von der Form a, von denen Q Nichtrest ist. Die Anzahl dieser sei gleich ψ,
4. in Factoren von der Form b, von denen Q Nichtrest ist. Die Anzahl dieser sei gleich ω.

Dann sieht man leicht, dass $p=\psi+\omega$, $p'=\chi+\psi$ ist.

Wenn nun P von der Form $\pm A$ ist, so wird $\chi+\omega$ und daher auch $\chi-\omega$ eine gerade Zahl sein; somit wird $p'=p+\chi-\omega\equiv p$ (mod. 2). Ist aber P von der Form $\pm B$, so findet man durch einen ähnlichen Schluss, dass die Zahlen p und p' nach dem Modul 2 incongruent sind.

IV. Dies wenden wir auf einzelne Fälle an. Ist zunächst sowohl P als Q von der Form $+A$, so wird nach Satz 1) $p\equiv q$ (mod. 2). Es ist aber auch $p'\equiv p$ (mod. 2), daher $p'\equiv q$ (mod. 2), was mit Satz 2) überein-

stimmt. — Analog wird, wenn P von der Form $-A$, Q von der Form $+A$ ist, $p \equiv q \pmod{2}$ nach dem soeben bewiesenen Satze 2). Hieraus folgt, da $p' \equiv p$ ist, auch $p' \equiv q$. Es ist somit auch Satz 5) bewiesen.

Auf dieselbe Weise leitet man Satz 7) aus 3), Satz 8) entweder aus 4) oder aus 7), Satz 9) aus 6) und aus demselben Satze auch Satz 10) her.

Strenger Beweis des Fundamentalsatzes.

135.

Durch den vorigen Artikel sind die Sätze des Artikels 133 zwar nicht bewiesen, es ist aber gezeigt worden, dass ihre Richtigkeit von der Richtigkeit des Fundamentalsatzes, die wir für den Augenblick vorausgesetzt haben, abhängt. Aus der Art der Ableitung geht aber hervor, dass jene Sätze für die Zahlen P, Q gelten, wofern nur der Fundamentalsatz für alle Combinationen der Primfactoren dieser Zahlen stattfindet, selbst wenn er allgemein nicht richtig sein sollte. Jetzt gehen wir also zum Beweise des Fundamentalsatzes selbst über und schicken demselben folgende Erklärung voraus:

Wir werden sagen, der Fundamentalsatz sei bis zu irgend einer Zahl M richtig, wenn er für zwei beliebige Primzahlen gilt, von denen keine M übersteigt.

In analoger Weise hat man es zu verstehen, wenn wir sagen, dass die Sätze der Artikel 131, 132, 133 bis zu irgend einer Grenze richtig seien. Man sieht aber leicht, dass, wenn die Richtigkeit des Fundamentalsatzes bis zu irgend einer Grenze feststeht, auch diese Sätze bis zu derselben Grenze stattfinden werden.

136.

Dass das Fundamentaltheorem für kleine Zahlen richtig ist, lässt sich leicht durch Induction nachweisen und so die Grenze bestimmen, bis zu welcher dasselbe sicher stattfindet. Wir nehmen an, dass diese Induction angestellt sei, doch ist es vollständig gleichgültig, bis wohin sie fortgesetzt ist. Es würde also genügen, wenn wir die Richtigkeit des Satzes nur bis zur Zahl 5 bestätigt hätten; dies wird aber durch eine einzige Beobachtung erledigt, da $+5N3$, $\pm 3N5$ ist.

Wenn nun der Fundamentalsatz nicht allgemein richtig wäre, so würde es eine Grenze T geben, bis zu welcher er gilt, so jedoch, dass er bis zu der nächstgrösseren Zahl $T+1$ nicht mehr gilt. Dies ist aber dasselbe, als wenn wir sagen, dass es zwei Primzahlen giebt, von denen die grössere $T+1$ ist und die mit einander verglichen dem Fundamentalsatze widersprechen, dass aber je zwei beliebige andere Primzahlen, wofern sie nur beide kleiner als $T+1$ sind, mit diesem Satze in Übereinstimmung sich befinden. Hieraus folgt, dass auch die Sätze der Artikel 131, 132, 133 bis zur Grenze T stattfinden werden. Wir werden aber jetzt zeigen, dass diese Annahme nicht bestehen kann. Je nach den verschiedenen Formen, welche

sowohl $T+1$ wie auch die Primzahl, welche kleiner als $T+1$ ist und die mit $T+1$ verglichen der Annahme nach dem Satze widerspricht, haben kann, müssen wir hierbei folgende Fälle unterscheiden. Jene Primzahl bezeichnen wir mit p.

Wenn sowohl $T+1$ als auch p von der Form $4n+1$ ist, so könnte der Fundamentalsatz auf zwiefache Weise unrichtig sein, nämlich wenn gleichzeitig wäre

entweder $\pm pR(T+1)$ und $\pm(T+1)Np$,
oder $\pm pN(T+1)$ und $\pm(T+1)Rp$.

Wenn sowohl $T+1$ als auch p von der Form $4n+3$ ist, so wird der Fundamentalsatz unrichtig sein, wenn gleichzeitig wäre

entweder $+pR(T+1)$ und $-(T+1)Np$
[oder was auf dasselbe hinauskommt: $-pN(T+1)$ und $+(T+1)Rp$]
oder $+pN(T+1)$ und $-(T+1)Rp$
[oder $-pR(T+1)$ und $+(T+1)Np$].

Wenn $T+1$ von der Form $4n+1$, p dagegen von der Form $4n+3$ ist, so ist der Fundamentalsatz unrichtig, wenn gleichzeitig wäre

entweder $\pm pR(T+1)$ und $+(T+1)Np$ [oder $-(T+1)Rp$]
oder $\pm pN(T+1)$ und $-(T+1)Np$ [oder $+(T+1)Rp$].

Wenn $T+1$ von der Form $4n+3$, p dagegen von der Form $4n+1$ ist, so ist der Fundamentalsatz unrichtig, wenn gleichzeitig wäre

entweder $+pR(T+1)$ [oder $-pN(T+1)$] und $\pm(T+1)Np$
oder $+pN(T+1)$ [oder $-pR(T+1)$] und $\pm(T+1)Rp$.

Wenn bewiesen werden kann, dass keiner dieser acht Fälle stattfinden kann, so sind wir zugleich sicher, dass die Richtigkeit des Fundamentalsatzes keinen Beschränkungen unterliegt. Diesen Beweis nehmen wir jetzt in Angriff. Da aber die einen von diesen Fällen von den andern abhängig sind, können wir nicht dieselbe Reihenfolge, in welcher wir sie hier aufgezählt haben, beibehalten.

137.

Erster Fall. Wenn $T+1$ von der Form $4n+1$ $(=a)$ und p von derselben Form, überdies aber noch $\pm pRa$ ist, so kann nicht $\pm aNp$ sein. Dieser Fall war oben der erste.

Es sei $+p \equiv e^2 \pmod{a}$ und e gerade und kleiner als a (was man immer erreichen kann). Dann sind zwei Fälle zu unterscheiden.

I. Wenn e durch p nicht teilbar ist, so setze man $e^2 = p + af$; dann wird f positiv, von der Form $4n+3$ (oder von der Form B), kleiner als a und durch p nicht teilbar sein. Ferner wird $e^2 \equiv p \pmod{f}$ sein, d. h. es ist pRf und daher nach dem Satze 11 des Artikel 132 (weil nämlich p

und f kleiner als a sind und für diese jene Sätze gelten) $\pm fRp$. Es ist aber auch $afRp$, mithin auch $\pm aRp$.

II. Wenn e durch p teilbar ist, so setze man $e = gp$ und $e^2 = p + aph$ oder $pg^2 = 1 + ah$. Dann ist h von der Form $4n + 3$ (B) und prim zu p und g^2. Ferner wird pg^2Rh und daher auch pRh, somit (nach Satz 11 Artikel 132) $\pm hRp$. Es ist aber auch $-ahRp$, weil $-ah \equiv 1$ (mod. p). Mithin wird auch $\pm aRp$ sein.

138.

Zweiter Fall. Wenn $T + 1$ von der Form $4n + 1$ ($= a$), p von der Form $4n + 3$ und $\pm pR$ ($T + 1$) ist, so kann nicht $+ (T + 1)$ Np oder $- (T + 1)$ Rp sein. Dieser Fall war oben der fünfte.

Es sei wie oben $e^2 = p + fa$ und e gerade und kleiner als a.

I. Wenn e durch p nicht teilbar ist, so wird auch f durch p nicht teilbar sein. Überdies aber wird f positiv, von der Form $4n + 1$ (oder A) und kleiner als a sein. Ferner ist $+ pRf$ und daher (Satz 10 Artikel 132) $+ fRp$. Es ist aber auch $+ faRp$; mithin wird $+ aRp$ oder $- aNp$.

II. Wenn e durch p teilbar ist, so sei $e = pg$ und $f = ph$. Es ist daher $g^2p = 1 + ha$. Sodann ist h positiv, von der Form $4n + 3$ (B) und prim zu p und g^2. Ferner $+ g^2pRh$ und somit $+ pRh$. Hiernach wird (Satz 13 Artikel 132) $- hRp$. Es ist aber $- haRp$, somit $+ aRp$ und $- aNp$.

139.

Dritter Fall. Wenn $T + 1$ von der Form $4n + 1$ ($= a$), p von derselben Form und $\pm pNa$ ist, so kann nicht $\pm aRp$ sein. (Oben der zweite Fall).

Man nehme irgend eine unterhalb a liegende Primzahl an, von welcher $+ a$ Nichtrest ist; dass es solche giebt, haben wir oben bewiesen (Artikel 125, 129). Wir müssen jedoch hier zwei Fälle gesondert betrachten, je nachdem diese Primzahl von der Form $4n + 1$ oder $4n + 3$ ist; denn es ist nicht bewiesen worden, dass es solche Primzahlen von jeder der beiden Formen giebt.

I. Es sei jene Primzahl von der Form $4n + 1$ und gleich a'. Dann ist $\pm a'Na$ (Artikel 131) und daher $\pm a'pRa$. Es sei also $e^2 \equiv a'p$ (mod. a) und e gerade und kleiner als a. Dann sind wieder vier Fälle zu unterscheiden.

1. Wenn e weder durch p noch durch a' teilbar ist, so setze man $e^2 = a'p \pm af$, wobei die Zeichen so zu nehmen sind, dass f positiv wird. Dann ist $f < a$, zu a' und p prim und für das obere Zeichen von der Form $4n + 3$, für das untere von der Form $4n + 1$. Der Kürze wegen wollen wir durch $[x, y]$ die Anzahl der Primfactoren der Zahl y, von denen x Nichtrest ist, bezeichnen. Dann ist $a'pRf$ und daher $[a'p, f] = 0$. Hiernach wird $[f, a'p]$ eine gerade Zahl (Satz 1 und 3 Artikel 133), d. h.

entweder gleich 0 oder gleich 2. Somit wird f Rest entweder von jeder oder von keiner der beiden Zahlen a', p. Jenes ist aber unmöglich, da $\pm af$ Rest von a' und $\pm aNa'$ (nach Voraussetzung) ist. Daher wird $\pm fNa'$. Demnach muss f Nichtrest von jeder der beiden Zahlen a', p sein. Wegen $\pm afRp$ aber wird $\pm aNp$, w. z. b. w.

2. Wenn e durch p aber nicht durch a' teilbar ist, so sei $e = gp$ und $g^2p = a' \pm ah$, wobei das Zeichen so bestimmt ist, dass h positiv wird. Dann ist $h < a$, zu a', g und p prim und für das obere Zeichen von der Form $4n+3$, für das untere aber von der Form $4n+1$. Aus der Gleichung $g^2p = a' \pm ah$ leitet man, nachdem sie durch p und a' multipliciert ist, ohne Schwierigkeit die folgenden Relationen her:

$$(\alpha)\quad pa'Rh; \qquad (\beta)\quad \pm ahpRa'; \qquad (\gamma)\quad aa'hRp.$$

Aus (α) folgt: $[pa', h] = 0$ und daher (Satz 1 und 3 Artikel 133) $[h, pa']$ gerade, d. h. es ist h entweder von jeder der beiden Zahlen p, a' Nichtrest oder von keiner. Im ersteren Falle folgt aus (β) $\pm apNa'$ und da nach Voraussetzung $\pm aNa'$ ist, so wird $\pm pRa'$. Hieraus ergiebt sich nach dem Fundamentalsatze, welcher für die unterhalb $T+1$ liegenden Zahlen p und a' gilt, $\pm a'Rp$. Hieraus und weil hNp ist, folgt nach (γ) $\pm aNp$, was bewiesen werden sollte. — In letzterem Falle folgt aus (β) $\pm apRa'$, somit $\pm pNa'$, $\pm a'Np$, und hieraus schliesslich und weil hRp ist, ergiebt sich nach (γ) $\pm aNp$.

3. Wenn e durch a' nicht aber durch p teilbar ist, so schreitet der Beweis fast auf dieselbe Weise fort, wie im vorhergehenden Falle, und kann keinem Schwierigkeiten bereiten, der diesen ganz durchdrungen hat.

4. Wenn e sowohl durch a' als durch p und daher auch durch das Product $a'p$ teilbar ist (denn wir nehmen an, dass die Zahlen a', p von einander verschieden sind, da sonst das, was wir beweisen wollen, nämlich, dass aNp ist, schon in der Voraussetzung aNa' enthalten wäre), so sei $e = ga'p$ und $g^2a'p = 1 \pm ah$. Dann wird $h < a$, zu a' und p prim und für das obere Zeichen von der Form $4n+3$, für das untere von der Form $4n+1$. Man sieht aber leicht, dass man aus jener Gleichung die folgenden Relationen herleiten kann:

$$(\alpha)\quad a'pRh; \qquad (\beta)\quad \pm ahRa'; \qquad (\gamma)\quad \pm ahRp.$$

Aus (α), welches mit (α) im zweiten Falle übereinstimmt, folgt wie dort, dass gleichzeitig entweder hRp und hRa' oder hNp und hNa' ist. Im ersteren Falle würde aber im Widerspruch mit der Voraussetzung infolge von (β) aRa' sein; somit ist hNp und daher nach (γ) auch aNp.

II. Wenn jene Primzahl von der Form $4n+3$ ist, so ist der Beweis dem vorigen so ähnlich, dass wir es für überflüssig halten, ihn herzusetzen. Für diejenigen, welche ihn für sich entwickeln wollen (was wir sehr empfehlen), bemerken wir nur, dass es, nachdem man zu einer solchen

Gleichung $e^2 = bp \pm af$ (wo b jene Primzahl bezeichnet) gekommen ist, die Deutlichkeit erhöhen wird, wenn jedes der beiden Vorzeichen gesondert betrachtet wird.

140.

Vierter Fall. Wenn $T+1$ von der Form $4n+1 (=a)$, p von der Form $4n+3$ und $\pm pNa$ ist, so kann nicht aRp oder $-aNp$ sein. (Oben der sechste Fall.)

Auch den Beweis dieses Falles lassen wir, da er dem Beweise des dritten Falles durchaus analog ist, der Kürze wegen fort.

141.

Fünfter Fall. Wenn $T+1$ von der Form $4n+3$ $(=b)$, p von derselben Form und $+pRb$ oder $-pNb$ ist, so kann nicht $+bRp$ oder $-bNp$ sein. (Oben der dritte Fall.)

Es sei $p \equiv e^2$ (mod. b) und e gerade und kleiner als b.

I. Ist e nicht durch p teilbar, so setze man $e^2 = p + bf$. Dann wird f positiv, von der Form $4n+3$, kleiner als b und prim zu p. Ferner wird pRf und daher nach Satz 13 Artikel 132: $-fRp$. Hieraus und aus $+bfRp$ wird $-bRp$ und daher $+bNp$.

II. Ist e durch p teilbar, so sei $e = pg$ und $g^2p = 1 + bh$. Dann wird h von der Form $4n+1$ und prim zu p, ferner $p \equiv g^2p^2$ (mod. h) und daher pRh sein. Hieraus wird $+hRp$ (Satz 10 Artikel 132) und hieraus sowie aus $-bhRp$ folgt $-bRp$ oder $+bNp$.

142.

Sechster Fall. Wenn $T+1$ von der Form $4n+3 (=b)$, p von der Form $4n+1$ und pRb ist, so kann nicht $\pm bNp$ sein. (Oben der siebente Fall.)

Den Beweis, der dem vorhergehenden vollkommen analog ist, lassen wir weg.

143.

Siebenter Fall. Wenn $T+1$ von der Form $4n+3 (=b)$, p von derselben Form und $+pNb$ oder $-pRb$ ist, so kann nicht $+bNp$ oder $-bRp$ sein. (Oben der vierte Fall.)

Es sei $-p \equiv e^2$ (mod. b) und e gerade und kleiner als b.

I. Ist e durch p nicht teilbar, so sei $-p = e^2 - bf$. Dann wird positiv, von der Form $4n+1$, zu p prim und kleiner als b (denn es ist sicher e nicht grösser als $b-1$ und $p < b-1$, daher $bf = e^2 + p < b^2 - b$ d. h. $f < b-1$). Ferner ist $-pRf$, somit (Satz 10 Artikel 132 $+fRp$ und hieraus sowie aus $+bfRp$ folgt $+bRp$ oder $-bNp$.

II. Wenn e durch p teilbar ist, so sei $e = pg$ und $g^2p = -1 + bh$. Dann wird h positiv, von der Form $4n+3$, zu p prim und kleiner als b.

Ferner wird $-pRh$, somit (Satz 14 Artikel 132) $+hRp$. Hieraus sowie aus $bhRp$ folgt $+bRp$ oder $-bNp$.

144.

Achter Fall. Ist $T+1$ von der Form $4n+3$ $(=b)$, p von der Form $4n+1$ und $+pNb$ oder $-pRb$, so kann nicht $\pm bRp$ sein. (Oben der letzte Fall.)

Der Beweis schreitet ebenso fort wie im vorhergehenden Falle.

Analoges Verfahren für den Beweis des Satzes im Artikel 114.

145.

In den vorhergehenden Beweisen haben wir für e stets einen geraden Wert angenommen (Artikel 137—144); wir bemerken, dass wir auch einen ungeraden Wert hätten anwenden können, doch hätten wir alsdann noch mehrere Unterscheidungen einführen müssen. Diejenigen, die an diesen Untersuchungen Gefallen finden, werden nichts Unnützliches thun, wenn sie ihre Kräfte an der Entwicklung dieser Fälle üben. Ausserdem hätten dann die auf die Reste $+2$ und -2 bezüglichen Sätze vorausgesetzt werden müssen. Da aber unser Beweis ohne diese Sätze durchgeführt worden ist, so erlangen wir dadurch ein neues Verfahren, jene Sätze zu beweisen. Dies ist keineswegs gering anzuschlagen, da die Methoden, deren wir uns oben für den Beweis des Satzes, dass ± 2 Rest einer jeden Primzahl von der Form $8n+1$ ist, bedient haben, weniger direct erscheinen könnten. Wir werden annehmen, dass die übrigen Fälle (welche sich auf die Primzahlen von den Formen $8n+3$, $8n+5$, $8n+7$ beziehen) nach den oben angeführten Methoden bewiesen und jener Satz nur durch Induction gefunden sei; diese Induction aber wollen wir durch die nachfolgenden Betrachtungen zur Gewissheit erheben.

Wenn ± 2 nicht von allen Primzahlen von der Form $8n+1$ Rest wäre, so setze man die kleinste Primzahl dieser Form, von welcher ± 2 Nichtrest ist, gleich a, so dass für alle Primzahlen, welche kleiner als a sind, der Satz gilt. Dann nehme man irgend eine Primzahl unterhalb $\frac{1}{2}a$ an, von welcher a Nichtrest ist (dass es solche giebt, folgt leicht aus Artikel 129). Ist diese gleich p, so wird nach dem Fundamentalsatze pNa. Hieraus wird $\pm 2pRa$. — Es sei daher $e^2 \equiv 2p$ (mod. a), so dass e ungerade und kleiner als a ist. Alsdann sind zwei Fälle zu unterscheiden.

Ist e nicht durch p teibar, so sei $e^2 = 2p + aq$. Dann ist q positiv, von der Form $8n+7$ oder von der Form $8n+3$ (je nachdem p von der Form $4n+1$ oder $4n+3$ ist), kleiner als a und durch p nicht teilbar. Jetzt teile man sämtliche Primfactoren von q in vier Klassen und zwar seien e von der Form $8n+1$, f von der Form $8n+3$, g von der Form $8n+5$ und h von der Form $8n+7$; das Product aus allen Factoren der ersten

Klasse sei E, die Producte aus den Factoren der zweiten, dritten, vierten Klasse respective F, G, H.*) Nachdem dies geschehen, betrachten wir zuerst den Fall, wo p von der Form $4n+1$ oder q von der Form $8n+7$ ist. Dann sieht man leicht, dass $2RE$, $2RH$ und daher pRE, pRH, und hieraus schliesslich ERp, HRp ist. Ferner wird 2 und daher auch p Nichtrest eines jeden Factors von der Form $8n+3$ oder $8n+5$; demnach ist jeder solcher Factor Nichtrest von p, woraus leicht folgt, dass FG Rest von p ist, wenn $f+g$ gerade, Nichtrest dagegen, wenn $f+g$ ungerade ist. Es kann aber $f+g$ nicht ungerade sein, denn man erkennt leicht durch Aufzählung aller Fälle, dass $EFGH$ oder q entweder von der Form $8n+3$ oder von der Form $8n+5$ wird, wenn $f+g$ ungerade ist, was auch sonst die einzelnen e, f, g, h sein mögen, und dies steht im Widerspruch mit der Voraussetzung. Es ist daher $FGRp$, $EFGHRp$ oder qRp und hieraus schliesslich, da $aqRp$ ist, aRp, gegen die Voraussetzung. — Ist zweitens p von der Form $4n+3$, so lässt sich auf ähnliche Weise zeigen, dass pRE und daher ERp, $-pRF$ und daher FRp, schliesslich $g+h$ gerade und demnach $GHRp$ ist, woraus schliesslich im Widerspruch mit der Voraussetzung folgt: qRp, aRp.

II. Ist e durch p teilbar, so lässt sich der Beweis in ähnlicher Weise führen und wird von Kundigen (für die allein dieser Artikel geschrieben ist) leicht entwickelt werden können. Wir lassen ihn der Kürze wegen fort.

Lösung des allgemeinen Problems.

146.

Durch das Fundamentaltheorem und die auf die Reste -1 und ± 2 bezüglichen Sätze lässt sich stets bestimmen, ob irgend eine gegebene Zahl Rest oder Nichtrest von einer gegebenen Primzahl ist. Es wird aber nicht unnützlich sein, auch das Andere, was wir oben auseinandergesetzt haben, hier nochmals vor Augen zu führen, damit man Alles, was zur Lösung des folgenden Problems nötig ist, beisammen habe.

Aufgabe. Wenn irgend zwei Zahlen P, Q gegeben sind, zu bestimmen, ob die eine Q Rest oder Nichtrest der andern P ist.

Auflösung I. Es sei $P = a^\alpha b^\beta c^\gamma \ldots$, wo $a, b, c, \ldots$ positiv genommene (denn P ist offenbar absolut zu nehmen) ungleiche Primzahlen bezeichnen. Der Kürze halber wollen wir in diesem Artikel einfach Relation zwischen zwei Zahlen x, y die Beziehung nennen, in welcher sie zu einander stehen, insofern die erste x Rest oder Nichtrest der zweiten y ist. Es hängt daher die Relation zwischen Q, P von den Relationen zwischen Q, a^α; Q, b^β u.s.w. ab (Artikel 105).

---

*) Wenn aus einer Klasse keine Factoren vorhanden wären, müsste man für das Product aus diesen 1 schreiben.

II. Um die Relation zwischen Q und a^α (von den andern Q, b^β, u. s. w. gilt nämlich dasselbe) kennen zu lernen, sind zwei Fälle zu unterscheiden.

1. Ist Q teilbar durch a, so setze man $Q = Q'a^e$, so dass Q' nicht mehr durch a teilbar ist. Ist dann $e = \alpha$ oder $e > \alpha$, so wird QRa^α; ist aber $e < \alpha$ und ungerade, so ist QNa^α; ist endlich $e < \alpha$ und gerade, so wird Q zu a^α dieselbe Relation haben wie Q' zu $a^{\alpha-e}$. Es ist daher dieser Fall zurückgeführt auf

2. wenn Q durch a nicht teilbar ist. Hierbei unterscheiden wir wiederum zwei Fälle.

(A) wenn $a = 2$ ist. Dann wird stets QRa^α, sobald $\alpha = 1$ ist; ist aber $\alpha = 2$, so ist erforderlich, dass Q von der Form $4n + 1$ sei; ist endlich $\alpha = 3$ oder $\alpha > 3$, so muss Q von der Form $8n + 1$ sein. Ist diese Bedingung erfüllt, so ist QRa^α.

(B) wenn a irgend eine andere Primzahl ist. Dann wird Q zu a^α dieselbe Relation haben, wie zu a (vgl. Artikel 101).

III. Die Relation irgend einer Zahl Q zu der (ungeraden) Primzahl a wird in folgender Weise ermittelt. Ist $Q > a$, so substituiere man für Q seinen kleinsten positiven Rest nach dem Modul a*). Dieser wird zu a dieselbe Relation haben wie Q.

Ferner zerlege man Q, oder die dafür genommene Zahl, in seine Primfactoren $p, p', p'', \ldots$, denen noch der Factor -1 hinzuzufügen ist, wenn Q negativ ist. Dann hängt bekanntlich die Relation zwischen Q und a von den Relationen zwischen den einzelnen Factoren $p, p', p'', \ldots$ und a ab. Wenn nämlich unter jenen Factoren $2m$ Nichtreste von a sind, so wird QRa, wenn aber $2m + 1$ vorhanden sind, so wird QNa. Man sieht aber leicht, dass, wenn unter den Factoren $p, p', p'', \ldots$ zwei oder vier oder sechs oder allgemein $2k$ gleiche vorkommen, diese sicher weggelassen werden können.

IV. Kommen -1 und 2 unter den Factoren $p, p', p'', \ldots$ vor, so kann deren Relation zu a aus den Artikeln 108, 112, 113, 114 bestimmt werden. Die Relation der übrigen zu a aber hängt von der Relation von a zu ihnen ab (Fundamentaltheorem und Sätze des Artikels 131). Ist p einer von ihnen, so wird man finden (indem man die Zahlen a, p ebenso behandelt wie vorher Q und a, die respective grösser als jene sind), dass die Relation von a zu p entweder nach den Artikeln 108—114 bestimmt werden kann (wenn nämlich der kleinste Rest von a nach dem Modul p keine ungeraden Primfactoren hat) oder noch überdies von der Relation von p zu gewissen Primzahlen, die kleiner als p sind, abhängt. Dasselbe gilt von den übrigen Factoren $p', p'', \ldots$ Man sieht nun leicht, dass man durch Fortsetzung dieses Verfahrens schliesslich zu Zahlen gelangen wird, deren Relationen nach den Sätzen der Artikel 108—114 bestimmt werden können. Durch ein Beispiel wird dies deutlicher werden.

---

*) Rest in der Bedeutung des Artikel 4. — Häufig ist es besser, den absolut kleinsten Rest zu nehmen.

Beispiel. Man sucht die Relation der Zahl $+453$ zu 1236. Es ist $1236 = 4 \cdot 3 \cdot 103$; $+453\, R 4$ nach II. 2. (A); $+453\, R 3$ nach II. 1. Es bleibt also noch die Relation von $+453$ zu 103 zu ermitteln. Sie wird dieselbe sein wie die, welche $+41$ $\left(\equiv 453 \,(\text{mod. } 103)\right)$ zu 103 hat. Diese wieder ist (nach dem Fundamentalsatz) dieselbe wie die von $+103$ zu 41 oder von -20 zu 41. Es ist aber $-20\, R\, 41$; denn es ist $-20 = -1 \cdot 2 \cdot 2 \cdot 5$; $-1\, R\, 41$ (Artikel 108) und $+5\, R\, 41$ deshalb, weil $41 \equiv 1$ und daher Rest von 5 ist (nach dem Fundamentalsatze). Hieraus folgt $+453\, R\, 103$ und hieraus schliesslich $+453\, R\, 1236$. In der That ist $453 \equiv 297^2 \,(\text{mod. } 1236)$.

Über die linearen Formen, welche sämtliche Primzahlen enthalten, von denen eine beliebige gegebene Zahl Rest oder Nichtrest ist.

147.

Ist eine beliebige Zahl A gegeben, so kann man bestimmte Formeln angeben, unter denen alle zu A primen Zahlen, von denen A Rest ist, enthalten sind, oder alle Zahlen enthalten sind, die Teiler der Zahlen von der Form $x^2 - A$ (wo x^2 ein unbestimmtes Quadrat bezeichnet) sein können.*) Der Kürze halber wollen wir nur diejenigen Teiler in Rücksicht ziehen, welche ungerade und prim zu A sind, da auf diese die übrigen Fälle leicht zurückgeführt werden können.

Es sei zunächst A entweder eine positive Primzahl von der Form $4n+1$ oder eine negative von der Form $4n-1$. Dann werden dem Fundamentalsatze zufolge alle Primzahlen, welche positiv genommen Reste von A sind, Teiler von $x^2 - A$, alle Primzahlen aber (mit Ausnahme der Zahl 2, welche immer Teiler ist), welche Nichtreste von A sind, Nichtteiler von $x^2 - A$ sein. Es seien alle Reste von A, welche kleiner als A sind, (mit Ausschluss der Null) bezeichnet mit $r, r', r'', \ldots$, alle Nichtreste dagegen mit $n, n', n'', \ldots$ Dann wird jede Primzahl, welche in einer der Formen $Ak + r$, $Ak + r'$, $Ak + r''$, ... enthalten ist, Teiler von $x^2 - A$, jede Primzahl aber, die in einer der Formen $Ak + n$, $Ak + n'$, $Ak + n''$, ... enthalten ist, Nichtteiler von $x^2 - A$ sein, wobei k eine unbestimmte ganze Zahl bezeichnet. Jene Formen nennen wir Formen der Teiler, diese aber Formen der Nichtteiler von $x^2 - A$. Die Anzahl jeder der beiden Arten ist gleich $\frac{1}{2}(A-1)$. Ist ferner B eine zusammengesetzte ungerade Zahl und ARB, so werden alle Primfactoren von B und daher auch B in irgend einer der ersteren Formen enthalten sein. Daher ist jede in der Form der Nichtteiler enthaltene ungerade Zahl Nichtteiler der

*) Derartige Zahlen werden wir einfach Teiler von $x^2 - A$ nennen, woraus von selbst hervorgeht, was Nichtteiler sind.

Form $x^2 - A$. Diesen Satz darf man aber nicht umkehren; denn wenn B ein zusammengesetzter ungerader Nichtteiler der Form $x^2 - A$ ist, wird es unter den Primfactoren von B einige Nichtteiler geben, und wenn die Anzahl dieser gerade ist, wird sich trotzdem B in irgend einer Form der Teiler vorfinden. Vgl. Artikel 99.

Beispiel. Auf diese Weise findet man für $A = -11$ als Formen der Teiler von $x^2 + 11$ die folgenden: $11k + 1, 3, 4, 5, 9$; die Formen der Nichtteiler aber sind: $11k + 2, 6, 7, 8, 10$. Es wird daher -11 Nichtrest aller ungeraden Zahlen, welche in irgend einer der letzteren Formen enthalten sind, Rest aber von allen zu irgend einer der ersteren Formen gehörigen Primzahlen sein.

Derartige Formen giebt es für die Teiler und Nichtteiler von $x^2 - A$, welche Zahl auch A bezeichnen möge. Man sieht aber leicht, dass man nur diejenigen Werte von A zu betrachten braucht, welche durch keine Quadratzahl teilbar sind; denn offenbar werden, wenn $A = a^2 A'$ ist, alle Teiler*) von $x^2 - A$ auch Teiler von $x^2 - A'$ sein, und dasselbe gilt von den Nichtteilern. — Wir werden aber drei Fälle unterscheiden: 1. wenn A von der Form $+(4n+1)$ oder $-(4n-1)$ ist; 2. wenn A von der Form $-(4n+1)$ oder $+(4n-1)$ ist; 3. wenn A gerade oder von der Form $\pm(4n+2)$ ist.

148.

Erster Fall, wenn A von der Form $+(4n+1)$ oder $-(4n-1)$ ist. Man zerlege A in seine Primfactoren und erteile denen, welche von der Form $4n+1$ sind, das positive, denen aber, welche von der Form $4n-1$ sind, das negative Vorzeichen (wodurch das Product gleich A wird). Diese Factoren seien $a, b, c, d, \ldots$ Man verteile ferner sämtliche Zahlen, welche kleiner als A und prim zu A sind, in zwei Klassen und zwar nehme man in die erste Klasse sämtliche Zahlen, welche entweder von keiner oder von zweien oder von vieren oder allgemein von einer geraden Anzahl der Zahlen $a, b, c, d, \ldots$ Nichtreste sind, in die zweite Klasse aber diejenigen, welche entweder von einer oder von dreien oder allgemein von einer ungeraden Anzahl der Zahlen $a, b, c, d, \ldots$ Nichtreste sind. Die ersteren bezeichne man mit $r, r', r'', \ldots$, die letzteren mit $n, n', n'', \ldots$ Dann werden die Formen $Ak + r, Ak + r', Ak + r'', \ldots$ die Formen der Teiler von $x^2 - A$, die Formen $Ak + n, Ak + n', Ak + n'', \ldots$ dagegen die Formen der Nichtteiler von $x^2 - A$ sein (d. h. jede Primzahl ausser 2 wird Teiler oder Nichtteiler von $x^2 - A$ sein, je nachdem sie in irgend einer der ersteren oder der letzteren Formen enthalten ist). Denn wenn p eine positive Primzahl und von irgend einer der Zahlen $a, b, c, \ldots$ Rest oder Nichtrest ist, so wird diese Zahl selbst Rest oder Nichtrest von p sein (nach dem Fundamentalsatz). Wenn es daher unter den Zahlen $a, b, c, \ldots$

*) Welche nämlich prim zu A sind.

m Zahlen giebt, von denen p Nichtrest ist, so wird es ebenso viele Nichtreste von p geben, und daher wird, wenn p in einer der ersteren Formen enthalten ist, m gerade und ARp, wenn es aber in einer der letzteren enthalten ist, m ungerade und ANp sein.

Beispiel. Es sei $A = +105 = -3 \times +5 \times -7$. Dann sind die Zahlen $r, r', r'', \ldots$ die folgenden: 1, 4, 16, 46, 64, 79 (welche Nichtreste von keiner der Zahlen 3, 5, 7 sind); 2, 8, 23, 32, 53, 92 (welche Nichtreste der Zahlen 3, 5 sind); 26, 41, 59, 89, 101, 104 (welche Nichtreste der Zahlen 3, 7 sind); 13, 52, 73, 82, 97, 103 (welche Nichtreste der Zahlen 5, 7 sind). — Die Zahlen $n, n', n'', \ldots$ aber sind die folgenden: 11, 29, 44, 71, 74, 86; 22, 37, 43, 58, 67, 88; 19, 31, 34, 61, 76, 94; 17, 38, 47, 62, 68, 83. Die sechs ersten sind Nichtreste von 3, die sechs ferneren Nichtreste von 5; dann folgen die Nichtreste von 7, schliesslich diejenigen, welche Nichtreste von allen dreien zugleich sind.

Aus der Lehre von den Combinationen und aus den Artikeln 32 und 96 leitet man leicht her, dass die Anzahl der Zahlen $r, r', r'', \ldots$ gleich

$$t\left(l + \frac{l(l-1)}{1 \cdot 2} + \frac{l(l-1)(l-2)(l-3)}{1 \cdot 2 \cdot 3 \cdot 4} + \cdots\right),$$

die Anzahl der Zahlen $n, n', n'', \ldots$ gleich

$$t\left(l + \frac{l(l-1)(l-2)}{1 \cdot 2 \cdot 3} + \frac{l(l-1)(l-2)(l-3)(l-4)}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} + \cdots\right)$$

ist, wobei l die Anzahl der Zahlen $a, b, c, \ldots$ bezeichnet,

$$t = 2^{-l}(a-1)(b-1)(c-1)\ldots$$

ist und jede der beiden Reihen soweit fortzusetzen ist, bis sie abbricht. (Es giebt nämlich t Zahlen, welche von allen Zahlen $a, b, c, \ldots$, $\frac{t \cdot l \cdot (l-1)}{1 \cdot 2}$ Zahlen, welche Nichtreste von zweien sind, u. s. w., doch gestattet das Streben nach Kürze nicht, diesen Beweis weitläufiger zu entwickeln). Die Summe jeder der beiden Reihen*) aber ist gleich 2^{l-1}. Die erste nämlich geht aus der folgenden

$$1 + (l-1) + \frac{(l-1)(l-2)}{1 \cdot 2} + \cdots$$

hervor, wenn man das zweite und dritte, das vierte und fünfte, u. s. w. Glied zusammennimmt, die letztere aber aus eben derselben Reihe, wenn man das erste und zweite, das dritte und vierte, u. s. w., Glied vereinigt.

---

*) Nach Fortlassung des Factors t.

Es giebt daher ebenso viele Formen der Teiler, wie Formen der Nichtteiler von $x^2 - A$, nämlich $\frac{1}{2}(a-1)(b-1)(c-1)\ldots$

149.

Den **zweiten** und **dritten Fall** können wir hier gleichzeitig betrachten. Es kann nämlich hier stets A entweder gleich $(-1)\,Q$ oder gleich $(+2)\,Q$ oder gleich $(-2)\,Q$ gesetzt werden, wo Q eine Zahl von der Form $+(4n+1)$ oder $-(4n-1)$, die wir im vorigen Artikel betrachtet haben, bezeichnet. Es sei allgemein $A = \alpha Q$, so dass α entweder gleich -1 oder gleich ± 2 ist. Dann ist A Rest aller Zahlen, von denen entweder jede oder keine der beiden Zahlen α und Q Rest ist, Nichtrest dagegen von allen Zahlen, von denen nur die eine der beiden Zahlen α und Q Nichtrest ist. Hieraus leitet man leicht die Formen der Teiler und Nichtteiler von $x^2 - A$ her. Ist $\alpha = -1$, so verteile man sämtliche Zahlen, welche kleiner als $4A$ und prim dazu sind, in zwei Klassen und zwar setze man in die erste Klasse diejenigen Zahlen, welche in irgend einer Form der Teiler von $x^2 - Q$ und zugleich in der Form $4n+1$ enthalten sind, und ferner diejenigen Zahlen, welche in irgend einer Form der Nichtteiler von $x^2 - Q$ und zugleich in der Form $4n+3$ enthalten sind, in die zweite Klasse aber die übrigen. Sind die ersteren $r, r', r'', \ldots$, die letzteren $n, n', n'' \ldots$, so ist A Rest von allen Primzahlen, welche in irgend einer der Formen $4Ak+r$, $4Ak+r'$, $4Ak+r''$, ... enthalten sind, Nichtrest dagegen von allen Primzahlen, welche in einer der Formen $4Ak+n$, $4Ak+n'$, ... enthalten sind. — Ist $\alpha = \pm 2$, so verteile man sämtliche Zahlen, welche kleiner als $8Q$ und prim dazu sind, in zwei Klassen und zwar setze man in die erste diejenigen Zahlen, welche in irgend einer Form der Teiler von $x^2 - Q$ und zugleich in einer der Formen $8n+1$, $8n+7$ für das obere Zeichen oder in einer der Formen $8n+3$, $8n+5$ für das untere Zeichen enthalten sind, und ferner diejenigen, welche in irgend einer Form der Nichtteiler von $x^2 - Q$ und zugleich in einer der Formen $8n+3$, $8n+5$ für das obere Zeichen oder in einer der Formen $8n+1$, $8n+7$ für das untere Zeichen enthalten sind; in die zweite Klasse aber die übrigen. Bezeichnet man sodann die Zahlen der ersten Klasse mit $r, r', r'', \ldots$, die der zweiten mit $n, n', n'', \ldots$, so wird $\pm 2Q$ Rest aller Primzahlen sein, welche in irgend einer der Formen $8Qk+r$, $8Qk+r'$, $8Qk+r''$, ... enthalten sind, Nichtrest dagegen von allen Primzahlen, welche in irgend einer der Formen $8Qk+n$, $8Qk+n'$, $8Qk+n''$, ... enthalten sind. Übrigens lässt sich leicht beweisen, dass es auch hier ebenso viele Formen der Teiler wie der Nichtteiler von $x^2 - A$ giebt.

Beispiel. Auf diese Weise findet man, dass $+10$ Rest von allen in irgend einer der Formen $40k+1$, 3, 9, 13, 27, 31, 37, 39 enthaltenen Primzahlen, dagegen Nichtrest von allen Primzahlen ist, welche in einer der Formen $40k+7$, 11, 17, 19, 21, 23, 29, 33 enthalten sind.

150.

Diese Formen haben mehrere ziemlich bemerkenswerte Eigenschaften, von denen wir jedoch nur eine anführen. Wenn B eine zusammengesetzte zu A prime Zahl ist, unter deren Primfactoren sich $2m$ befinden, welche in irgend einer Form der Nichtteiler von $x^2 - A$ enthalten sind, so wird B in irgend einer Form der Teiler von $x^2 - A$ enthalten sein; wenn dagegen die Anzahl der Primfactoren von B, welche in irgend einer Form der Nichtteiler von $x^2 - A$ enthalten sind, ungerade ist, so wird auch B in einer Form der Nichtteiler enthalten sein. Den Beweis, der nicht schwierig ist, lassen wir fort. Hieraus folgt aber, nicht nur dass jede Primzahl, sondern auch, dass jede zusammengesetzte ungerade zu A prime Zahl, welche in irgend einer Form der Nichtteiler enthalten ist, ein Nichtteiler ist; denn notwendigerweise muss irgend ein Primfactor einer solchen Zahl ein Nichtteiler sein.

Über die Arbeiten Anderer bezüglich dieser Untersuchungen.

151.

Das Fundamentaltheorem, welches sicherlich zu den elegantesten Entdeckungen auf diesem Gebiete zu rechnen ist, ist in derselben einfachen Form, in der wir es oben gegeben haben, bisher von Niemand ausgesprochen worden. Dies ist um so mehr zu verwundern, da gewisse andere aus ihm fliessende Sätze, von denen man leicht wieder zu jenem hätte zurückgelangen können, schon Euler bekannt waren. Dass es gewisse Formen giebt, in denen alle Primzahldivisoren der Zahlen von der Form $x^2 - A$ enthalten sind, und andere, in denen alle primen Nichtteiler der Zahlen von derselben Form enthalten sind und zwar so, dass diese jene ausschliessen, hatte er gewusst und ein Verfahren ermittelt, jene Formen zu finden; doch sind alle seine Versuche, zu einem Beweise zu gelangen, stets vergeblich gewesen und hatten nur jene durch Induction gefundene Wahrheit noch wahrscheinlicher gemacht. Zwar scheint er in einer Abhandlung, *Novae demonstrationes circa divisores numerorum formae* $x^2 + ny^2$, welche in den Schriften der Akademie zu Petersburg unterm 20. November 1775 erwähnt und nach dem Tode des ausgezeichneten Mannes im ersten Bande der *Nova Acta* dieser Akademie auf Seite 47 u. ff. aufbewahrt worden ist, geglaubt zu haben, dass der Beweis ihm geglückt sei; doch hat sich hier ein Irrtum eingeschlichen, da er Seite 65 stillschweigend annimmt, dass derartige Formen der Teiler und Nichtteiler existieren,*) woraus es

*) Nämlich dass es Zahlen $r, r', r'', \ldots, n, n', n'' \ldots$ giebt, die alle verschieden, kleiner als $4A$ und von solcher Beschaffenheit sind, dass alle primen Teiler von $x^2 - A$ unter irgend einer der Formen $4Ak + r$, $4Ak + r'$, ..., alle primen Nichtteiler dagegen unter irgend einer der Formen $4Ak + n$, $4Ak + n'$, ... enthalten sind (wo k eine unbestimmte Zahl bezeichnet).

nicht schwierig war abzuleiten, welcher Art sie sein mussten. Die Methode aber, deren er sich zur Glaubhaftmachung jener Annahme bediente, scheint nicht zweckentsprechend zu sein. In einer andern Abhandlung: *De criteriis aequationis* $fx^2+gy^2=hz^2$ *utrumque resolutionem admittat necne, Opusc. Anal. T. I* (wo f, g, h gegebene, x, y, z unbestimmte Zahlen sind) fand er durch Induction, dass, wenn die Gleichung für irgend einen Wert $h=s$ auflösbar ist, dieselbe auch für jeden andern mit s nach dem Modul $4fg$ congruenten Wert, wofern derselbe eine Primzahl ist, auflösbar ist, ein Satz, aus welchem die in Rede stehende Annahme ohne Schwierigkeit bewiesen werden kann. Aber auch der Beweis dieses Satzes spottete allen seinen Anstrengungen*), was nicht zu verwundern ist, da man nach unserer Meinung vom Fundamentaltheorem ausgehen musste. Übrigens wird die Richtigkeit dieses Satzes aus dem, was wir im folgenden Abschnitt darlegen werden, von selbst sich ergeben.

Nach Euler beschäftigte sich Legendre mit demselben Gegenstande in der ausgezeichneten Abhandlung *Recherches d'analyse indéterminée, Hist. de l'Ac. des Sc. 1785, p. 465 u. ff.* Er gelangt hierin (Seite 465) zu dem Satze, der, was die Sache selbst betrifft, mit dem Fundamentaltheorem identisch ist, nämlich dass, wenn p und q zwei positive Primzahlen bezeichnen, die absolut kleinsten Reste der Potenzen $p^{\frac{q-1}{2}}$ und $q^{\frac{p-1}{2}}$ nach den Moduln q, p respective entweder beide $+1$ oder beide -1 sind, wenn entweder p oder q von der Form $4n+1$ ist; dass aber, wenn sowohl p als auch q von der Form $4n+3$ ist, der eine absolut kleinste Rest $+1$, der andere -1 ist, woraus nach Artikel 106 folgt, dass die Relation (in der im Artikel 146 angenommenen Bedeutung) von p zu q und von q zu p dieselbe ist, wenn entweder p oder q von der Form $4n+1$ ist, dagegen entgegengesetzt, wenn sowohl p als auch q von der Form $4n+3$ ist. Dieser Satz ist unter den Sätzen des Artikel 131 enthalten; er folgt auch aus den Sätzen 1, 3, 9 des Artikels 133; umgekehrt aber lässt sich auch das Fundamentaltheorem daraus ableiten. Legendre hat auch den Beweis versucht, über den wir, da er äusserst geistreich ist, im folgenden Abschnitt weitläufiger sprechen werden. Da er aber in demselben manches ohne Beweis angenommen hat (wie er Seite 520 selbst gesteht: *Nous avons supposé seulement etc.*), was zum Teil bisher noch von Niemand bewiesen

---

*) Wie er selbst gesteht, a. a. O. S. 216: „*Hujus elegantissimi theorematis demonstratio adhuc desideratur, postquam a pluribus jamdudum frustra est investigata ... Quocirca plurimum is praestitisse censendus est, cui successerit demonstrationem hujus theorematis invenire*". — Mit welcher Begier der unsterbliche Mann nach dem Beweise dieses Satzes und anderer, welche nur specielle Fälle des Fundamentaltheorems sind, verlangt hat, ist aus vielen anderen Stellen der *Opusc. Analyt.* zu ersehen. Vgl. *Additamentum ad diss. VIII, T. I* und *diss. XIII, T. II* und mehrere Abhandlungen in den *Comment. Ac. Petrop.*, die wir bereits erwähnt haben.

worden ist, zum Teil, nach unserer Ansicht wenigstens, ohne das Fundamentaltheorem nicht bewiesen werden kann, so scheint der von ihm eingeschlagene Weg nicht zum Ziele führen zu können und muss daher unserer Beweis für den ersten gehalten werden.*) — Übrigens werden wir weiter unten zwei andere Beweise desselben höchst wichtigen Satzes mitteilen, die von dem vorigen und unter sich völlig verschieden sind. Cf. pg. 449

Über die nichtreinen Congruenzen zweiten Grades.

152.

Bisher haben wir die reine Congruenz $x^2 \equiv A$ (mod. m) behandelt und gezeigt, wie man entscheiden kann, ob sie lösbar ist. Die Ermittlung der Wurzeln selbst ist durch Artikel 105 auf den Fall zurückgeführt worden, wo m entweder eine Primzahl oder die Potenz einer Primzahl ist, der letztere Fall aber durch Artikel 101 wiederum auf den, wo m eine Primzahl ist. Für diesen Fall aber umfasst das, was wir in dem Artikel 61 u. ff. mitgeteilt haben, zusammen mit dem, was wir im fünften und achten Abschnitt darlegen werden, beinahe alles, was sich durch directe Methoden ermitteln lässt. Diese sind aber, wo sie überhaupt anwendbar sind, meistens unendlich viel weitläufiger als die indirecten, die wir im sechsten Abschnitt auseinandersetzen werden, und daher nicht sowohl wegen ihres praktischen Nutzens als vielmehr wegen ihrer Schönheit bemerkenswert.

Die nichtreinen Congruenzen zweiten Grades lassen sich leicht auf reine zurückführen. Ist die Congruenz

$$ax^2 + bx + c \equiv 0,$$

welche nach dem Modul m gelöst werden soll, vorgelegt, so ist mit derselben die folgende äquivalent:

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{4am},$$

d. h. jede Zahl, welche der einen genügt, wird auch der andern genügen. Diese lässt sich aber folgendermassen darstellen:

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{4am},$$

woraus alle Werte von $2ax + b$, welche kleiner als $4am$ sind, wenn es deren giebt, gefunden werden können. Bezeichnet man dieselben mit $r, r', r'', \ldots,$

*) Vgl. die Zusätze am Schlusse der *Disquisitiones.*

so werden alle Lösungen der gegebenen Congruenz sich aus den Lösungen der Congruenzen

$$2ax \equiv r - b, \quad 2ax \equiv r' - b, \ \ldots \quad (\text{mod. } 4am),$$

die wir im Abschnitt II finden lehrten, ergeben. Übrigens bemerken wir, dass die Auflösung meistenteils durch verschiedene Kunstgriffe zusammengezogen, z. B. an Stelle der gegebenen Congruenz eine mit ihr gleichbedeutende

$$a'x^2 + 2b'x + c' \equiv 0$$

gefunden werden kann, in welcher a' in m aufgeht; doch gestattet die Kürze nicht, dies hier weitläufiger zu entwickeln, und kann man darüber den letzten Abschnitt vergleichen.

Fünfter Abschnitt.

Von den Formen und unbestimmten Gleichungen zweiten Grades.

Gegenstand der Untersuchung; Definition der Formen und Bezeichnung.

153.

In diesem Abschnitte werden wir insbesondere von den Functionen zweier Unbestimmten x, y von folgender Form

$$ax^2 + 2bxy + cy^2,$$

wo a, b, c gegebene ganze Zahlen sind, handeln und werden dieselben **Formen** zweiten Grades oder einfach **Formen** nennen. Diese Untersuchung gipfelt in der Lösung des berühmten Problems, alle Lösungen irgend einer unbestimmten Gleichung zweiten Grades mit zwei Unbekannten zu finden, sei es nun, dass diese Unbekannten ganze oder nur rationale Werte erhalten sollen. Dieses Problem ist zwar schon von Lagrange gelöst und vieles auf die Natur der Formen Bezügliche sowohl von diesem grossen Geometer als auch von Euler teils zuerst gefunden, teils, nachdem es von Fermat gefunden, bewiesen worden. Bei einer gründlichen Untersuchung der Formen hat sich uns aber so viel Neues dargeboten, dass es der Mühe wert erschien, den ganzen Gegenstand von Neuem vorzunehmen, um so mehr, als das von jenen Männern Gefundene an vielen Stellen zerstreut und nach unserer Erfahrung nur wenigen bekannt geworden ist, sodann weil die Art der Behandlung dieses Gegenstandes zum grössten Teil uns eigen ist, endlich weil das von uns Herrührende ohne neue Darlegung des Früheren kaum verständlich sein würde. Doch dürfte es nicht zweifelhaft sein, dass noch vieles Ausgezeichnete in dieser Beziehung verborgen geblieben ist, an dem andere ihre Kräfte üben können. Übrigens werden wir das auf die Geschichte der hervorragendsten Eigenschaften Bezügliche stets an der geeigneten Stelle anführen.

Die Form $ax^2 + 2bxy + cy^2$ werden wir, sobald es sich nicht um die Unbestimmten x, y handelt, durch (a, b, c) bezeichnen. Dieser Ausdruck wird also unbestimmt die Summe dreier Teile bezeichnen, nämlich des Products der gegebenen Zahl a in das Quadrat einer beliebigen Unbestimmten, des doppelten Products der Zahl b in diese Unbestimmte und in eine andere Unbestimmte und endlich des Products der Zahl c in das Quadrat dieser zweiten Unbestimmten. Z. B. wird $(1, 0, 2)$ die Summe eines Quadrates und eines doppelten Quadrates darstellen. Obwohl ferner die Formen (a, b, c) und (c, b, a) dasselbe bezeichnen, wenn wir nur auf die Teile selbst Rücksicht nehmen, so werden sie sich doch unterscheiden, wenn wir überdies auf die Reihenfolge der Teile achten. Wir werden sie daher in der Folge sorgfältig unterscheiden; was wir daraus für Vorteil haben, wird aus dem Nachstehenden hinreichend klar werden.

Darstellung der Zahlen; die Determinante.

154.

Wir sagen, irgend eine gegebene Zahl werde durch eine gegebene Form **dargestellt**, wenn den Unbestimmten der Form solche ganzzahligen Werte beigelegt werden, dass der Wert der Form der gegebenen Zahl gleich wird. Hier haben wir den folgenden

Satz. Wenn sich die Zahl M so durch die Form (a, b, c) darstellen lässt, dass die Werte der Unbestimmten, durch welche dies bewirkt wird, prim zu einander sind, so wird $b^2 - ac$ quadratischer Rest der Zahl M sein.

Beweis. Sind die Werte der Unbestimmten m, n, also

$$am^2 + 2bmn + cn^2 = M,$$

und nimmt man zwei Zahlen μ, ν von solcher Beschaffenheit an, dass $\mu m + \nu n = 1$ ist (Artikel 40), so zeigt man durch Entwicklung leicht, dass

$$(am^2 + 2bmn + cn^2)(a\nu^2 - 2b\mu\nu + c\mu^2) = [\mu(mb + nc) - \nu(ma + nb)]^2 - (b^2 - ac)(m\mu + n\nu)^2$$

oder

$$M(a\nu^2 - 2b\mu\nu + c\mu^2) = [\mu(mb + nc) - \nu(ma + nb)]^2 - (b^2 - ac)$$

ist. Daher ist:

$$b^2 - ac \equiv [\mu(mb + nc) - \nu(ma + bn)]^2 \pmod{M},$$

d. h. es ist $b^2 - ac$ quadratischer Rest von M.

Die Zahl $b^2 - ac$, von deren Beschaffenheit, wie wir im Folgenden zeigen werden, die Eigenschaften der Form (a, b, c) hauptsächlich abhängen, werden wir die **Determinante** dieser Form nennen.

Die Werte des Ausdrucks $\sqrt{b^2-ac}$ (mod. M), zu welchen die Darstellung der Zahl M durch die Form (a, b, c) gehört.

155.

Es ist somit

$$\mu(mb+nc)-\nu(ma+nb)$$

ein Wert des Ausdrucks

$$\sqrt{b^2-ac}\,(\text{mod. } M).$$

Bekanntlich aber können auf unzählig viele Weisen Zahlen μ, ν derart bestimmt werden, dass $\mu m+\nu n=1$ ist, so dass andere und andere Werte jenes Ausdrucks sich ergeben werden. Wir wollen zusehen, in welchem Zusammenhang diese unter einander stehen. Es sei nicht nur $\mu m+\nu n=1$, sondern auch $\mu' m+\nu' n=1$, und man setze:

$$\mu(mb+nc)-\nu(ma+nb)=v,\quad \mu'(mb+nc)-\nu'(ma+nb)=v'.$$

Multipliciert man die Gleichung $\mu m+\nu n=1$ mit μ', die andere $\mu' m+\nu' n=1$ mit μ, und subtrahiert sie, so wird $\mu'-\mu=n(\mu'\nu-\mu\nu')$, und analog wird, wenn man jene mit ν', diese mit ν multipliciert und subtrahiert: $\nu'-\nu=m(\mu\nu'-\mu'\nu)$. Hieraus folgt sogleich:

$$v'-v=(\mu'\nu-\mu\nu')(am^2+2bmn+cn^2)=(\mu'\nu-\mu\nu')M$$

oder $v'\equiv v$ (mod. M). Auf welche Art also auch μ, ν bestimmt sein mögen, die Formel $\mu(mb+nc)-\nu(ma+nb)$ kann keine verschiedenen (d. i. incongruenten) Werte des Ausdrucks $\sqrt{b^2-ac}$ (mod. M) ergeben. Wenn daher v irgend ein Wert jener Formel ist, so werden wir sagen, die Darstellung der Zahl M durch diejenige Form $ax^2+2bxy+cy^2$, in welcher $x=m$, $y=n$ ist, gehöre zum Werte v des Ausdrucks $\sqrt{b^2-ac}$ (mod. M). Übrigens kann man leicht zeigen, dass, wenn v irgend ein Wert jener Formel und $v'\equiv v$ (mod. M) ist, man an Stelle der Zahlen μ, ν, welche v geben, andere μ', ν' nehmen kann, welche v' geben. Denn macht man:

$$\mu'=\mu+\frac{n(v'-v)}{M},\quad \nu'=\nu-\frac{m(v'-v)}{M},$$

so wird

$$\mu' m+\nu' n=\mu m+\nu n=1,$$

der aus μ', ν' sich ergebende Wert der Formel aber wird den aus μ, ν hervorgehenden um die Grösse $(\mu'\nu-\mu\nu')M$, welche gleich $(\mu m+\nu n)(v'-v)$ $=v'-v$ wird, übersteigen, d. h. jener Wert wird gleich v' sein.

156.

Wenn man zwei Darstellungen derselben Zahl M durch dieselbe Form (a, b, c) hat, in welchen die Unbestimmten zu einander prime Werte haben, so können dieselben entweder zu demselben Werte des Ausdrucks $\sqrt{b^2 - ac}$ (mod. M) gehören oder zu verschiedenen. Ist

$$M = am^2 + 2bmn + cn^2 = am'^2 + 2bm'n' + cn'^2$$

und

$$\mu m + \nu n = 1, \quad \mu' m' + \nu' n' = 1,$$

so wird offenbar, wenn

$$\mu(mb + nc) - \nu(ma + nb) \equiv \mu'(m'b + n'c) - \nu'(m'a + n'b) \pmod{M}$$

war, diese Congruenz stets bestehen bleiben, welche andern passenden Werte für μ, ν; μ', ν' auch genommen werden; in diesem Falle werden wir sagen, dass beide Darstellungen zu demselben Werte des Ausdrucks $\sqrt{b^2 - ac}$ (mod. M) gehören. Wenn aber jene Congruenz für irgend welche Werte von μ, ν; μ', ν' nicht stattfindet, so wird sie überhaupt für keine stattfinden und dann werden die Darstellungen zu verschiedenen Werten gehören. Und wenn

$$\mu(mb + nc) - \nu(ma + nb) \equiv -[\mu'(m'b + n'c) - \nu'(m'a + n'b)]$$

ist, so soll gesagt werden, dass die Darstellungen zu entgegengesetzten Werten des Ausdrucks $\sqrt{b^2 - ac}$ gehören. Aller dieser Benennungen werden wir uns auch bedienen, wenn es sich um mehrere Darstellungen derselben Zahl durch verschiedene Formen, die jedoch dieselbe Determinante haben, handelt.

Beispiel. Die gegebene Form sei $(3, 7, -8)$, deren Determinante gleich 73 ist. Mit Hülfe dieser Form hat man folgende Darstellungen der Zahl 57:

$$3 \cdot 13^2 + 14 \cdot 13 \cdot 25 - 8 \cdot 25^2; \qquad 3 \cdot 5^2 + 14 \cdot 5 \cdot 9 - 8 \cdot 9^2.$$

Für die erste kann man $\mu = 2$, $\nu = -1$ setzen und erhält dadurch als Wert des Ausdruckes $\sqrt{73}$ (mod. 57), zu welchem die Darstellung gehört:

$$2(13 \cdot 7 - 25 \cdot 8) + (13 \cdot 3 + 25 \cdot 7) = -4.$$

Auf ähnliche Weise findet man, indem man $\mu = 2$, $\nu = -1$ setzt, dass die zweite Darstellung zum Werte $+4$ gehört. Daher gehören die beiden Darstellungen zu entgegengesetzten Werten.

Bevor wir weiter gehen, bemerken wir, dass die Formen, deren Determinante gleich Null ist, von den folgenden Untersuchungen ganz ausgeschlossen werden, da sie nur die Kürze der Sätze stören würden und daher eine gesonderte Behandlung erfordern.

Form, welche eine andere enthält oder unter einer anderen enthalten ist; Transformation, eigentliche und uneigentliche.

157.

Wenn eine Form F, deren Unbestimmten x, y sind, in eine andere F', deren Unbestimmten x', y' sind, durch Substitutionen von der Form

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y',$$

in denen α, β, γ, δ ganze Zahlen sind, übergeführt werden kann, so werden wir sagen, dass die erstere die letztere **enthalte** oder dass die letztere unter der ersteren **enthalten** sei. Ist F die Form:

$$ax^2 + 2bxy + cy^2,$$

die Form F' aber die folgende:

$$a'x'^2 + 2b'x'y' + c'y'^2,$$

so hat man folgende drei Gleichungen:

$$a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2,$$
$$b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta,$$
$$c' = a\beta^2 + 2b\beta\delta + c\delta^2.$$

Multipliciert man die zweite Gleichung mit sich selbst, die erste mit der dritten und subtrahiert, so erhält man nach Weglassung der sich aufhebenden Teile:

$$b'^2 - a'c' = (b^2 - ac)(\alpha\delta - \beta\gamma)^2.$$

Hieraus folgt, dass die Determinante der Form F' durch die Determinante der Form F teilbar und der Quotient ein Quadrat ist; offenbar werden also diese Determinanten dasselbe Vorzeichen besitzen. Wenn daher überdies die Form F' durch eine ähnliche Substitution in die Form F verwandelt werden kann, d. h. wenn sowohl F' unter F als auch F unter F' enthalten ist, werden die Determinanten der Formen einander gleich*) und $(\alpha\delta - \beta\gamma)^2 = 1$ sein. In diesem Falle nennen wir die Formen **äquivalent**. Demnach ist zur Äquivalenz der Formen die Gleichheit der Determinanten unerlässliche Bedingung, obwohl jene aus dieser allein keineswegs folgt. Die Substitution $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ werden wir eine **eigentliche** Transformation nennen, wenn $\alpha\delta - \beta\gamma$ eine **positive** Zahl, und eine **uneigentliche**, wenn $\alpha\delta - \beta\gamma$ eine **negative** Zahl ist; von der Form F' werden wir sagen, sie sei **eigentlich** oder **uneigentlich** unter der Form F **enthalten**, wenn F sich durch eine eigentliche oder uneigentliche Transformation in die

---

*) Aus vorstehender Analyse geht hervor, dass dieser Satz auch für Formen, deren Determinante gleich Null ist, gilt. Aber die Gleichung $(\alpha\delta - \beta\gamma)^2 = 1$ darf nicht auf diesen Fall ausgedehnt werden.

Form F' verwandeln lässt. Wenn daher die Formen F und F' äquivalent sind, so ist $(\alpha\delta - \beta\gamma)^2 = 1$ und daher, wenn die Transformation eine eigentliche ist, $\alpha\delta - \beta\gamma = +1$, wenn sie eine uneigentliche ist, $\alpha\delta - \beta\gamma = -1$. — Wenn mehrere Transformationen zu gleicher Zeit eigentlich oder zu gleicher Zeit uneigentlich sind, so werden wir sie **gleichartig** nennen, eine eigentliche und eine uneigentliche dagegen sollen **ungleichartig** heissen.

Äquivalenz, eigentliche und uneigentliche.

158.

Wenn die Determinanten der Formen F, F' einander gleich sind und F' unter F enthalten ist, so wird auch F unter F' enthalten sein und zwar eigentlich oder uneigentlich, je nachdem F' unter F eigentlich oder uneigentlich enthalten ist.

Es möge F in F' übergehen, wenn man setzt:

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'.$$

Dann wird F' in F übergehen durch

$$x' = \delta x - \beta y, \quad y' = -\gamma x + \alpha y,$$

denn offenbar wird durch diese Substitution aus F' dasselbe, was aus F wird, wenn man setzt:

$$x = \alpha(\delta x - \beta y) + \beta(-\gamma x + \alpha y), \quad y = \gamma(\delta x - \beta y) + \delta(-\gamma x + \alpha y)$$

oder

$$x = (\alpha\delta - \beta\gamma)x, \quad y = (\alpha\delta - \beta\gamma)y.$$

Hiernach wird aus F offenbar $(\alpha\delta - \beta\gamma)^2 F$, d. i. wiederum F (nach vorigem Artikel). Es ist aber ersichtlich, dass die letztere Transformation eigentlich oder uneigentlich ist, je nachdem die erstere eigentlich oder uneigentlich ist.

Wenn sowohl F' unter F als auch F unter F' eigentlich enthalten ist, werden wir die Formen **eigentlich äquivalent**, wenn sie aber uneigentlich unter einander enthalten sind, **uneigentlich äquivalent** nennen. — Im Übrigen wird man den Nutzen dieser Unterscheidungen bald kennen lernen.

Beispiel. Die Form $2x^2 - 8xy + 3y^2$ geht durch die Substitutionen $x = 2x' + y'$, $y = 3x' + 2y'$ über in die Form: $-13x'^2 - 12x'y' - 2y'^2$ und diese wieder in jene, wenn man setzt: $x' = 2x - y$, $y' = -3x + 2y$. Daher sind die Formen $(2, -4, 3)$ und $(-13, -6, -2)$ eigentlich äquivalent.

Die **Probleme, an deren Behandlung wir jetzt gehen**, sind die folgenden:

I. Wenn irgend zwei Formen mit derselben Determinante gegeben sind, so soll man ermitteln, ob sie äquivalent sind oder nicht, ob eigentlich

oder uneigentlich äquivalent oder beides zugleich, denn auch dieses ist möglich. Wenn sie aber verschiedene Determinanten haben, so soll man zusehen, ob nicht wenigstens die eine die andere, eigentlich oder uneigentlich oder in beiderlei Weise, enthält. Schliesslich soll man alle, eigentlichen sowohl wie uneigentlichen, Transformationen der einen in die andere finden.

II. Wenn irgend eine Form gegeben ist, so soll man finden, ob eine gegebene Zahl durch sie dargestellt werden kann, und soll alle Darstellungen angeben. Da aber hierbei die Formen mit negativer Determinante ein anderes Verfahren erfordern als die Formen mit positiver Determinante, so wollen wir zunächst das angeben, was beiden gemeinsam ist, und darauf die Formen jeder Art gesondert betrachten.

Entgegengesetzte Formen.

159.

Wenn die Form F die Form F' und diese wiederum die Form F'' enthält, so wird die Form F ebenfalls die Form F'' enthalten.

Es seien die Unbestimmten der Formen F, F', F'' respective x, y; x', y'; x'', y'', und es möge F in F' übergehen, wenn man setzt:

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y',$$

und F' in F'', wenn man setzt:

$$x' = \alpha' x'' + \beta' y'', \quad y' = \gamma' x'' + \delta' y''.$$

Dann wird sich offenbar F in F'' verwandeln durch

$$x = \alpha(\alpha' x'' + \beta' y'') + \beta(\gamma' x'' + \delta' y''), \quad y = \gamma(\alpha' x'' + \beta' y'') + \delta(\gamma' x'' + \delta' y'')$$

oder:

$$x = (\alpha\alpha' + \beta\gamma') x'' + (\alpha\beta' + \beta\delta') y'', \quad y = (\gamma\alpha' + \delta\gamma') x'' + (\gamma\beta' + \delta\delta') y''.$$

Somit wird F auch F'' enthalten.

Da

$$(\alpha\alpha' + \beta\gamma')(\gamma\beta' + \delta\delta') - (\alpha\beta' + \beta\delta')(\gamma\alpha' + \delta\gamma') = (\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma')$$

und daher positiv ist, wenn entweder $\alpha\delta - \beta\gamma$ und $\alpha'\delta' - \beta'\gamma'$ beide positiv oder beide negativ sind, dagegen negativ, wenn eine dieser Zahlen positiv, die andere negativ ist, so wird die Form F die Form F'' eigentlich oder uneigentlich enthalten, je nachdem F die Form F' und F' wieder die Form F'' auf einerlei oder auf verschiedene Weise enthalten.

Hieraus folgt, dass, wenn man beliebig viele Formen F, F', F'', F''', ... hat, von denen jede die folgende enthält, die erste die letzte enthalten wird, und zwar eigentlich, wenn die Anzahl der Formen, welche die ihnen folgende uneigentlich enthalten, gerade, uneigentlich, wenn jene Anzahl ungerade ist.

Wenn die Form F der Form F' und diese wieder der Form F'' äquivalent ist, so wird die Form F der Form F'' äquivalent sein, und zwar eigentlich, wenn die Form F der Form F' in derselben Weise äquivalent ist, wie die Form F' der Form F'', uneigentlich aber, wenn letzteres in verschiedener Weise der Fall ist.

Denn da die Formen F, F' respective den Formen F', F'' äquivalent sind, so werden nicht nur jene diese respective enthalten und daher auch F die Form F'', sondern auch diese jene. Daher werden F und F'' äquivalent sein. Aus dem Vorhergehenden aber folgt, dass F die Form F'' eigentlich oder uneigentlich enthält, je nachdem F der Form F' und F' der Form F'' auf dieselbe oder auf verschiedene Weise äquivalent ist; ebenso wird auch F'' die Form F enthalten. Daher werden im ersteren Falle F und F'' eigentlich, im letzteren uneigentlich äquivalent sein.

Die Formen $(a, -b, c)$, (c, b, a), $(c, -b, a)$ sind der Form (a, b, c) äquivalent, und zwar die beiden ersten uneigentlich, die letzte eigentlich.

Denn $ax^2 + 2bxy + cy^2$ geht in $ax'^2 - 2bx'y' + cy'^2$ über, wenn man setzt $x = x' + 0 \cdot y'$, $y = 0 \cdot x' - y'$, und diese Transformation ist uneigentlich wegen $1 \cdot (-1) - 0 \cdot 0 = -1$. In die Form $cx'^2 + 2bx'y' + cy'^2$ aber geht sie über durch die uneigentliche Transformation: $x = 0 \cdot x' + y'$, $y = x' + 0 \cdot y'$, und in die Form $cx'^2 - 2bx'y' + ay'^2$ durch die eigentliche Transformation $x = 0 \cdot x' - y'$, $y = x' + 0 \cdot y'$.

Hieraus ist klar, dass jede Form, welche der Form (a, b, c) äquivalent ist, entweder dieser selbst oder der Form $(a, -b, c)$ eigentlich äquivalent ist, und ebenso dass, wenn irgend eine Form die Form (a, b, c) enthält oder unter ihr enthalten ist, dieselbe entweder die Form (a, b, c) oder die Form $(a, -b, c)$ eigentlich enthält, oder unter einer von beiden eigentlich enthalten ist. Die Formen (a, b, c) und $(a, -b, c)$ werden wir **entgegengesetzte** nennen.

Benachbarte Formen.

160.

Wenn die Formen (a, b, c) und (a', b', c') dieselbe Determinante haben und überdies $c = a'$ und $b \equiv -b' \pmod{c}$ oder $b + b' \equiv 0 \pmod{c}$ ist, so werden wir diese Formen **benachbarte** Formen nennen, und zwar soll, wenn eine genauere Bestimmung nötig ist, die erste der letzteren **nach links benachbart**, die letztere der ersteren **nach rechts benachbart** heissen.

So ist z. B. die Form $(7, 3, 2)$ der Form $(3, 4, 7)$ nach rechts benachbart, die Form $(3, 1, 3)$ der zu ihr entgegengesetzten Form $(3, -1, 3)$ aber nach beiden Seiten benachbart.

Benachbarte Formen sind stets eigentlich äquivalent. Denn die Form $ax^2 + 2bxy + cy^2$ geht in die benachbarte Form $cx'^2 + 2b'x'y' + c'y'^2$ über durch die Substitution $x = -y'$, $y = x' + \frac{b+b'}{c}y'$ (welche wegen $0 \cdot \frac{b+b'}{c} - 1 \cdot (-1) = 1$ eine eigentliche ist), wie man durch Entwicklung mit Zuhülfenahme der Gleichung $b^2 - ac = b'^2 - cc'$ leicht beweist; $\frac{b+b'}{c}$ aber ist nach Voraussetzung eine ganze Zahl. — Übrigens gelten diese Erklärungen und Folgerungen nicht, wenn $c = a' = 0$ ist. Dieser Fall kann jedoch nur bei Formen eintreten, deren Determinante eine Quadratzahl ist.

Die Formen (a, b, c) und (a', b', c') sind eigentlich äquivalent, wenn $a = a'$, $b \equiv b'$ (mod. a) ist. Denn die Form (a, b, c) ist (nach vorigem Artikel) der Form $(c, -b, a)$ eigentlich äquivalent, letztere aber ist der Form (a', b', c') nach links benachbart.

Gemeinschaftliche Teiler der Coefficienten der Formen.

161.

Wenn die Form (a, b, c) die Form (a', b', c') enthält, so ist jeder gemeinschaftliche Teiler der Zahlen a, b, c auch ein Teiler der Zahlen a', b', c', und jeder gemeinschaftliche Teiler der Zahlen $a, 2b, c$ auch ein solcher von $a', 2b', c'$.

Wenn nämlich die Form $ax^2 + 2bxy + cy^2$ durch die Substitutionen $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ in die Form $a'x'^2 + 2b'x'y' + c'y'^2$ übergeht, so hat man folgende Gleichungen:

$$a\alpha^2 + 2b\alpha\gamma + c\gamma^2 = a'$$
$$a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b'$$
$$a\beta^2 + 2b\beta\delta + c\delta^2 = c',$$

woraus der Satz sogleich folgt (wenn man für den zweiten Teil desselben an Stelle der zweiten Gleichung die folgende anwendet: $2a\alpha\beta + 2b(\alpha\delta + \beta\gamma) + 2c\gamma\delta = 2b'$).

Hieraus geht hervor, dass der grösste gemeinschaftliche Teiler der Zahlen a, b $(2b)$, c zugleich auch in dem grössten gemeinschaftlichen Teiler der Zahlen a', b' $(2b')$, c' aufgeht. Wenn nun überdies die Form (a', b', c') die Form (a, b, c) enthält, d. h. wenn die Formen äquivalent sind, so wird der grösste gemeinschaftliche Teiler der Zahlen a, b $(2b)$, c dem grössten gemeinschaftlichen Teiler der Zahlen a', b' $(2b')$, c' gleich sein, da alsdann sowohl dieser in jenem, wie jener in diesem aufgehen muss. Wenn daher in diesem Falle die Zahlen a, b $(2b)$, c keinen gemeinschaftlichen Teiler haben, d. h. wenn der grösste gemeinsame Teiler gleich 1 ist, so werden auch die Zahlen a', b' $(2b')$, c' keinen gemeinschaftlichen Teiler besitzen.

Zusammenhang zwischen sämtlichen gleichartigen Transformationen einer gegebenen Form in eine gegebene Form.

162.

Aufgabe. Wenn die Form

$$AX^2 + 2BXY + CY^2 \text{ oder } F$$

die Form

$$ax^2 + 2bxy + cy^2 \text{ oder } f$$

enthält und irgend eine Transformation jener in diese gegeben ist, so soll man aus dieser alle andern ihr gleichartigen Transformationen ableiten.

Auflösung. Die gegebene Transformation sei die folgende: $X = \alpha x + \beta y$, $Y = \gamma x + \delta y$, und es werde zunächst angenommen, dass eine andere dieser gleichartige, nämlich $X = \alpha' x + \beta' y$, $Y = \gamma' x + \delta' y$, gegeben sei, um zuzusehen, was hieraus folgt. Setzt man die Determinanten der Formen F, f gleich D, d und $\alpha\delta - \beta\gamma = e$, $\alpha'\delta' - \beta'\gamma' = e'$, so wird (nach Artikel 157) $d = De^2 = De'^2$ und, da die Grössen e und e' nach Voraussetzung dasselbe Vorzeichen haben, $e = e'$. Man hat aber die folgenden sechs Gleichungen:

[1] $$A\alpha^2 + 2B\alpha\gamma + C\gamma^2 = a,$$
[2] $$A\alpha'^2 + 2B\alpha'\gamma' + C\gamma'^2 = a,$$
[3] $$A\alpha\beta + B(\alpha\delta + \beta\gamma) + C\gamma\delta = b,$$
[4] $$A\alpha'\beta' + B(\alpha'\delta' + \beta'\gamma') + C\gamma'\delta' = b,$$
[5] $$A\beta^2 + 2B\beta\delta + C\delta^2 = c,$$
[6] $$A\beta'^2 + 2B\beta'\delta' + C\delta'^2 = c.$$

Bezeichnen wir der Kürze wegen die Zahlen

$$A\alpha\alpha' + B(\alpha\gamma' + \gamma\alpha') + C\gamma\gamma',$$
$$A(\alpha\beta' + \beta\alpha') + B(\alpha\delta' + \beta\gamma' + \gamma\beta' + \delta\alpha') + C(\gamma\delta' + \delta\gamma'),$$
$$A\beta\beta' + B(\beta\delta' + \delta\beta') + C\delta\delta'$$

mit a', $2b'$, c', so leiten wir aus vorstehenden Gleichungen die folgenden her*):

[7] $$a'^2 - D(\alpha\gamma' - \gamma\alpha')^2 = a^2,$$
[8] $$2a'b' - D(\alpha\gamma' - \gamma\alpha')(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha') = 2ab,$$
$$4b'^2 - D[(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 + 2ee'] = 2b^2 + 2ac,$$

*) Diese Gleichungen entstehen folgendermassen: [7] entsteht aus [1]·[2] (d. h. wenn die Gleichung [1] mit der Gleichung [2] multipliciert wird, oder vielmehr, wenn die linke Seite jener mit der linken Seite dieser und die rechte Seite jener mit der rechten Seite dieser multipliciert wird und die Producte gleichgesetzt werden); [8] entsteht aus [1]·[4] + [2]·[3], die folgende nicht numerierte aus [1]·[6] + [2]·[5] + [3]·[4] + [3]·[4]; die folgende nicht numerierte aus [3]·[4], [11] aus [3]·[6] + [4]·[5]; [12] aus [5]·[6]. Einer ähnlichen Bezeichnung wie hier werden wir uns auch im Folgenden immer bedienen. Die Entwicklung müssen wir aber dem Leser überlassen.

und hieraus wird, wenn man $2Dee' = 2d = 2b^2 - 2ac$ addiert:

[9] $$4b'^2 - D(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 = 4b^2,$$
$$a'c' - D(\alpha\delta' - \gamma\beta')(\beta\gamma' - \delta\alpha') = b^2,$$

und aus dieser wird, wenn man $D(\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma') = b^2 - ac$ subtrahiert:

[10] $$a'c' - D(\alpha\gamma' - \gamma\alpha')(\beta\delta' - \delta\beta') = ac,$$
[11] $$2b'c' - D(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')(\beta\delta' - \delta\beta') = 2bc,$$
[12] $$c'^2 - D(\beta\delta' - \delta\beta')^2 = c^2.$$

Man nehme nun an, dass der grösste gemeinschaftliche Teiler der Zahlen a, $2b$, c gleich m sei und dass die Zahlen $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ so bestimmt seien, dass

$$\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m$$

wird (Artikel 40); man multipliciere sodann die Gleichungen [7], [8], [9], [10], [11], [12] respective mit $\mathfrak{A}^2$, $2\mathfrak{A}\mathfrak{B}$, $\mathfrak{B}^2$, $2\mathfrak{A}\mathfrak{C}$, $2\mathfrak{B}\mathfrak{C}$, $\mathfrak{C}^2$ und addiere die Producte. Setzt man noch der Kürze halber:

[13] $$\mathfrak{A}a' + 2\mathfrak{B}b' + \mathfrak{C}c' = T$$
[14] $$\mathfrak{A}(\alpha\gamma' - \gamma\alpha') + \mathfrak{B}(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha') + \mathfrak{C}(\beta\delta' - \delta\beta') = U,$$

wo T und U augenscheinlich ganze Zahlen sind, so erhält man die Gleichung:

$$T^2 - DU^2 = m^2.$$

Wir sind daher zu folgendem eleganten Schlusse gelangt, nämlich dass sich aus irgend zwei gleichartigen Transformationen der Form F in f die Auflösung der unbestimmten Gleichung $t^2 - Du^2 = m^2$ in ganzen Zahlen, nämlich $t = T$, $u = U$, ergiebt. Da wir ferner bei unsern Schlussfolgerungen nicht angenommen haben, dass die Transformationen verschieden seien, so muss sogar eine einzige Transformation zweimal angewendet eine Lösung darbieten. Dann wird aber wegen $\alpha' = \alpha$, $\beta' = \beta, \ldots$ auch $a' = a$, $b' = b$, $c' = c$ und daher $T = m$, $U = 0$, eine Lösung, die unmittelbar auf der Hand liegt.

Jetzt wollen wir die erste Transformation und die Auflösung der unbestimmten Gleichung als bekannt betrachten und zusehen, wie man daraus die andere Transformation ableiten könne, oder in welcher Weise α', β', γ', δ' von α, β, γ, δ, T, U abhängen. Zu dem Zwecke multipliciere man zunächst die Gleichung [1] mit $\delta\alpha' - \beta\gamma'$, [2] mit $\alpha\delta' - \gamma\beta'$, [3] mit $\alpha\gamma' - \gamma\alpha'$, [4] mit $\gamma\alpha' - \alpha\gamma'$ und addiere die Producte. Dadurch entsteht die Gleichung:

[15] $$(e + e')a' = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')a.$$

Auf analoge Weise entsteht aus

$$(\delta\beta' - \beta\delta')([1] - [2]) + (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')([3] + [4]) + (\alpha\gamma' - \gamma\alpha')([5] - [6])$$

die Gleichung:

[16] $$2(e + e')b' = 2(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')b.$$

Endlich geht aus

$$(\delta\beta'-\beta\delta')([3]-[4])+(\alpha\delta'-\gamma\beta')[5]+(\delta\alpha'-\beta\gamma')[6]$$

die Gleichung hervor:

[17] $$(e+e')c'=(\alpha\delta'-\beta\gamma'-\gamma\beta'+\delta\alpha')c.$$

Substituiert man die Werte [15], [16], [17] in [13], so wird:

$$(e+e')T=(\alpha\delta'-\beta\gamma'-\gamma\beta'+\delta\alpha')(\mathfrak{A}a+2\mathfrak{B}b+\mathfrak{C}c)$$

oder:

[18] $$2eT=(\alpha\delta'-\beta\gamma'-\gamma\beta'+\delta\alpha')m,$$

woraus T viel leichter abgeleitet werden kann als aus [13]. — Verbindet man diese Gleichung mit [15], [16], [17], so erhält man: $ma'=Ta$, $2mb'=2Tb$, $mc'=Tc$. Werden diese Werte von a', $2b'$, c' in die Gleichungen [7] bis [12] eingesetzt und wird an Stelle von T^2 geschrieben m^2+DU^2, so gehen jene Gleichungen nach den gehörigen Änderungen über in die folgenden:

$$(\alpha\gamma'-\gamma\alpha')^2m^2=a^2U^2$$
$$(\alpha\gamma'-\gamma\alpha')(\alpha\delta'+\beta\gamma'-\gamma\beta'-\delta\alpha')m^2=2abU^2$$
$$(\alpha\delta'+\beta\gamma'-\gamma\beta'-\delta\alpha')^2m^2=4b^2U^2$$
$$(\alpha\gamma'-\delta\alpha')(\beta\delta'-\delta\beta')m^2=acU^2$$
$$(\alpha\delta'+\beta\gamma'-\gamma\beta'-\delta\alpha')(\beta\delta'-\delta\beta')m^2=2bcU^2$$
$$(\beta\delta'-\delta\beta')^2m^2=c^2U^2.$$

Hieraus leitet man mit Hülfe der Gleichung [14] und der Gleichung $\mathfrak{A}a+2\mathfrak{B}b+\mathfrak{C}c=m$ leicht her (indem man einmal die erste, zweite und vierte, sodann die zweite, dritte und fünfte, schliesslich die vierte, fünfte und sechste bezüglich mit $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ multipliciert und die Producte addiert):

$$(\alpha\gamma'-\gamma\alpha')Um^2=maU^2$$
$$(\alpha\delta'+\beta\gamma'-\gamma\beta'-\delta\alpha')Um^2=2mbU^2$$
$$(\beta\delta'-\delta\beta')Um^2=mcU^2,$$

und hieraus, indem man durch mU dividiert:*)

[19] $$aU=(\alpha\gamma'-\gamma\alpha')m$$
[20] $$2bU=(\alpha\delta'+\beta\gamma'-\gamma\beta'-\delta\alpha')m$$
[21] $$cU=(\beta\delta'-\delta\beta')m,$$

und aus irgend einer dieser Gleichungen lässt sich U viel leichter ableiten als aus [14]. — Zu gleicher Zeit folgt hieraus, dass, wie immer auch $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ bestimmt sein mögen (was auf unendlich viele Arten geschehen kann), sowohl T als auch U denselben Wert erhalten.

---

*) Dies würde nicht gestattet sein, wenn $U=0$ wäre; dann würde aber die Richtigkeit der Gleichungen [19], [20], [21] sogleich aus der ersten, dritten und sechsten der vorstehenden Gleichungen sich ergeben.

Multipliciert man nun die Gleichung [18] mit α, [19] mit 2β, [20] mit $-\alpha$, so ergiebt sich durch Addition:

$$2\alpha eT + 2(\beta a - \alpha b)U = 2(\alpha\delta - \beta\gamma)\alpha' m = 2e\alpha' m.$$

Auf analoge Weise wird aus $\beta\cdot[18] + \beta\cdot[20] - 2\alpha\cdot[21]$:

$$2\beta eT + 2(\beta b - \alpha c)U = 2(\alpha\delta - \beta\gamma)\beta' m = 2e\beta' m.$$

Ferner wird aus $\gamma\cdot[18] + 2\delta\cdot[19] - \gamma\cdot[20]$:

$$2\gamma eT + 2(\delta a - \gamma b)U = 2(\alpha\delta - \beta\gamma)\gamma' m = 2e\gamma' m.$$

Schliesslich ergiebt sich aus $\delta\cdot[18] + \delta\cdot[20] - 2\gamma\cdot[21]$:

$$2\delta eT + 2(\delta b - \gamma c)U = 2(\alpha\delta - \beta\gamma)\delta' m = 2e\delta' m.$$

Werden in diesen Formeln für a, b, c ihre Werte aus [1], [3], [5] gesetzt, so folgt:

$$\begin{aligned}\alpha' m &= \alpha T - (\alpha B + \gamma C)U\\ \beta' m &= \beta T - (\beta B + \delta C)U\\ \gamma' m &= \gamma T + (\alpha A + \gamma B)U\\ \delta' m &= \delta T + (\beta A + \delta B)U.\text{*)}\end{aligned}$$

Aus der vorstehenden Untersuchung folgt, dass es keine der gegebenen gleichartige Transformation der Form F in f giebt, die nicht unter der Formel

$$\text{(I)}\quad \begin{aligned}X &= \frac{1}{m}[\alpha t - (\alpha B + \gamma C)u]\,x + \frac{1}{m}[\beta t - (\beta B + \delta C)u]\,y,\\ Y &= \frac{1}{m}[\gamma t + (\alpha A + \gamma B)u]\,x + \frac{1}{m}[\delta t + (\beta A + \delta B)u]\,y\end{aligned}$$

enthalten wäre, wobei t und u unbestimmt alle ganzen Zahlen bezeichnen, welche der Gleichung $t^2 - Du^2 = m^2$ genügen. Hieraus können wir jedoch noch nicht schliessen, dass sämtliche Werte von t, u, welche jener Gleichung genügen, in die Formel (I) substituiert passende Transformationen geben. Es kann jedoch mit Hülfe der Gleichungen [1], [3], [5] und der Gleichung $t^2 - Du^2 = m^2$ durch Entwicklung leicht bestätigt werden:

1. dass die Form F durch eine aus irgend welchen Werten von t, u hervorgegangene Substitution stets in die Form f transformiert werden kann. Die mehr weitläufige als schwierige Rechnung unterdrücken wir der Kürze halber.

2. Jede aus der Formel abgeleitete Transformation ist der gegebenen gleichartig. Denn es ist:

---

*) Hieraus folgt leicht:
$$\begin{aligned}AeU &= (\delta\gamma' - \gamma\delta')m,\\ 2BeU &= (\alpha\delta' - \delta\alpha' + \gamma\beta' - \beta\gamma')m,\\ CeU &= (\beta\alpha' - \alpha\beta')m.\end{aligned}$$

$$\frac{1}{m}[\alpha t-(\alpha B+\gamma C)u]\times\frac{1}{m}[\delta t+(\beta A+\delta B)u]$$
$$-\frac{1}{m}[\beta t-(\beta B+\delta C)u]\times\frac{1}{m}[\gamma t+(\alpha A+\gamma B)u]$$
$$=\frac{1}{m^2}(\alpha\delta-\beta\gamma)(t^2-Du^2)=\alpha\delta-\beta\gamma.$$

3. Besitzen die Formen F und f ungleiche Determinanten, so kann es geschehen, dass die Formel (I) für irgend welche Werte von t und u Substitutionen ergiebt, welche Brüche enthalten, und die daher verworfen werden müssen. Alle andern aber werden passende Transformationen sein, und andere ausser ihnen giebt es nicht.

4. Wenn aber die Formen F und f dieselbe Determinante besitzen und daher äquivalent sind, so wird die Formel (I) keine Transformationen ergeben, welche Brüche enthalten, und wird somit in diesem Falle die vollständige Lösung der Aufgabe darstellen. Jenes aber wird folgendermassen bewiesen:

Aus dem Satze des vorigen Artikels folgt in diesem Falle, dass m zu gleicher Zeit gemeinschaftlicher Teiler der Zahlen A, $2B$, C ist. Da $t^2-Du^2=m^2$ ist, so wird $t^2-B^2u^2=m^2-ACu^2$; somit ist $t^2-B^2u^2$ durch m^2 teilbar und hiernach um so mehr $4t^2-4B^2u^2$, und somit ist auch (weil $2B$ durch m teilbar ist) $4t^2$ durch m^2 und folglich $2t$ durch m teilbar. Hiernach sind $\frac{2}{m}(t+Bu)$ und $\frac{2}{m}(t-Bu)$ ganze Zahlen und zwar (da die Differenz zwischen ihnen $\frac{4}{m}Bu$ gerade ist) entweder beide gerade oder beide ungerade. Wenn beide ungerade wären, würde auch ihr Product ungerade sein, welches aber als Vierfaches der Zahl $\frac{1}{m^2}(t^2-B^2u^2)$, die, wie wir eben gezeigt haben, eine ganze Zahl ist, notwendig gerade ist. Daher ist dieser Fall unmöglich; also sind $\frac{2}{m}(t+Bu)$, $\frac{2}{m}(t-Bu)$ immer gerade und daher $\frac{1}{m}(t+Bu)$, $\frac{1}{m}(t-Bu)$ immer ganz. Hieraus leitet man aber ohne Mühe her, dass alle vier Coefficienten in (I) stets ganze Zahlen sind.

Aus dem Vorstehenden schliesst man, dass, wenn man sämtliche Lösungen der Gleichung $t^2-Du^2=m^2$ hat, sich daraus alle Transformationen der Form (A, B, C) in die Form (a, b, c), welche der gegebenen Transformation gleichartig sind, ableiten lassen. Jene werden wir aber im Folgenden finden lehren. Hier bemerken wir nur, dass die Anzahl der Lösungen stets endlich ist, wenn D negativ oder positiv und zugleich eine Quadratzahl ist, dass sie aber unendlich gross ist, wenn D eine positive nichtquadratische Zahl ist. Wenn dieser Fall stattfindet und zugleich D nicht gleich d ist (oben 3), müsste man überdies untersuchen, auf welche Weise man diejenigen Werte von t, u, welche von Brüchen freie Sub-

stitutionen ergeben, von vornherein von denjenigen unterscheiden könne, welche gebrochene Substitutionen hervorbringen. Indessen werden wir für diesen Fall unten eine andere Methode auseinandersetzen, welche von diesem Übelstande frei ist (Artikel 214).

Beispiel. Die Form $x^2 + 2y^2$ geht durch die eigentliche Substitution $x = 2x' + 7y'$, $y = x' + 5y'$ in die Form (6, 24, 99) über; es werden alle eigentlichen Transformationen jener Form in diese gesucht. Hier ist $D = -2$, $m = 3$ und daher die zu lösende Gleichung $t^2 + 2u^2 = 9$. Dieser geschieht auf sechs verschiedene Arten Genüge, nämlich wenn man setzt: $t = 3, -3, 1, -1, 1, -1$; $u = 0, 0, 2, 2, -2, -2$ respective. Die dritte und sechste Lösung geben Substitutionen in gebrochenen Zahlen und sind daher zu verwerfen; aus den übrigen ergeben sich vier Substitutionen:

$$x = \begin{cases} 2x' + 7y' \\ -2x' - 7y' \\ -2x' - 9y' \\ 2x' + 9y' \end{cases} \qquad y = \begin{cases} x' + 5y' \\ -x' - 5y' \\ x' + 3y' \\ -x' - 3y', \end{cases}$$

deren erste die gegebene ist.

Ambige Formen.

163.

Bereits oben haben wir oberflächlich erwähnt, dass es möglich sei, dass irgend eine Form F eine andere F' sowohl eigentlich als auch uneigentlich enthält. Offenbar tritt dies ein, wenn zwischen die Formen F, F' eine andere G von der Beschaffenheit eingeschoben werden kann, dass F die Form G und G die Form F' enthält und G sich selbst uneigentlich äquivalent ist. Denn wenn man annimmt, dass F die Form G eigentlich oder uneigentlich enthalte, so wird, da G die Form G uneigentlich enthält, F die Form G bezüglich uneigentlich oder eigentlich enthalten und daher in beiden Fällen sowohl eigentlich als auch uneigentlich (Artikel 159). In derselben Weise leitet man hieraus ab, dass, wie man auch immer annehmen möge, dass G die Form F' enthalte, F immer F' sowohl eigentlich als auch uneigentlich enthalten muss. — Dass es aber solche Formen giebt, welche sich selbst uneigentlich äquivalent sind, ersieht man aus dem ganz auf der Hand liegenden Falle, wo das mittlere Glied der Form gleich Null ist. Eine solche Form ist sich nämlich selbst entgegengesetzt (Artikel 159) und daher uneigentlich äquivalent. Allgemeiner besitzt jede Form (a, b, c), in welcher $2b$ durch a teilbar ist, diese Eigenschaft. Dieser wird nämlich die Form (c, b, a) nach links benachbart (Artikel 160) und daher eigentlich äquivalent sein; (c, b, a) aber ist nach Artikel 159 der Form (a, b, c) n-eigentlich äquivalent; somit ist (a, b, c) sich selbst uneigentlich äquivalent. Derartige Formen (a, b, c), in denen $2b$ durch a teilbar ist, werden wir **ambige** Formen nennen. Wir haben daher folgenden

Satz. Die Form F wird eine andere Form F' sowohl eigentlich als uneigentlich enthalten, wenn man eine ambige Form finden kann, welche unter F enthalten ist und F' enthält.

Dieser Satz lässt sich aber auch umkehren, nämlich:

Satz betreffend den Fall, wo eine Form unter einer andern zugleich eigentlich und uneigentlich enthalten ist.

164.

Satz. Wenn die Form

$$Ax^2 + 2Bxy + Cy^2 \text{ oder } F$$

eine andere Form

$$A'x'^2 + 2B'x'y' + C'y'^2 \text{ oder } F'$$

sowohl eigentlich als auch uneigentlich enthält, so lässt sich immer eine ambige Form finden, welche unter der Form F enthalten ist und die Form F' enthält.

Wir nehmen an, dass die Form F in die Form F' sowohl durch die Substitution

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

als auch durch die folgende jener ungleichartige

$$x = \alpha' x' + \beta' y', \quad y = \gamma' x' + \delta' y'$$

übergehe. Bezeichnet man dann die Zahlen $\alpha\delta - \beta\gamma$, $\alpha'\delta' - \beta'\gamma'$ bezüglich mit e, e', so wird $B'^2 - A'C' = e^2(B^2 - AC) = e'^2(B^2 - AC)$, und hieraus $e^2 = e'^2$ und, da nach Voraussetzung e und e' entgegengesetzte Vorzeichen haben, $e = -e'$ oder $e + e' = 0$. Wenn man nun in F' für x' setzte $\delta' x'' - \beta' y''$ und für y': $-\gamma' x'' + \alpha' y''$, so würde offenbar dieselbe Form entstehen, als wenn man in F schriebe

entweder 1) für x: $\alpha(\delta' x'' - \beta' y'') + \beta(-\gamma' x'' + \alpha' y'')$
d. i. $(\alpha\delta' - \beta\gamma')x'' + (\beta\alpha' - \alpha\beta')y''$
und für y: $\gamma(\delta' x'' - \beta' y'') + \delta(-\gamma' x'' + \alpha' y'')$
d. i. $(\gamma\delta' - \delta\gamma')x'' + (\delta\alpha' - \gamma\beta')y''$
oder 2) für x: $\alpha'(\delta' x'' - \beta' y'') + \beta'(-\gamma' x'' + \alpha' y'')$ d. i. $e'x''$
und für y: $\gamma'(\delta' x'' - \beta' y'') + \delta'(-\gamma' x'' + \alpha' y'')$ d. i. $e'y''$.

Bezeichnet man daher die Zahlen $\alpha\delta' - \beta\gamma'$, $\beta\alpha' - \alpha\beta'$, $\gamma\delta' - \delta\gamma'$, $\delta\alpha' - \gamma\beta'$ mit a, b, c, d, so wird die Form F durch die beiden Substitutionen

$$x = ax'' + by'', \quad y = cx'' + dy''; \quad x = e'x'', \quad y = e'y''$$

in dieselbe Form verwandelt, wodurch man die drei folgenden Gleichungen erhält:

$$[1] \qquad Aa^2 + 2Bac + Cc^2 = Ae'^2$$
$$[2] \qquad Aab + B(ad + bc) + Ccd = Be'^2$$
$$[3] \qquad Ab^2 + 2Bbd + Cd^2 = Ce'^2.$$

Aus den Werten von a, b, c, d aber findet man:

$$[4] \qquad ad - bc = ee' = -e^2 = -e'^2.$$

Hiernach wird aus $d \cdot [1] - c \cdot [2]$:

$$(Aa + Bc)(ad - bc) = (Ad - Bc)e'^2$$

und daher:

$$A(a + d) = 0.$$

Ferner wird aus $(a + d) \cdot [2] - b \cdot [1] - c \cdot [3]$:

$$[Ab + B(a + d) + Cc](ad - bc) = [-Ab + B(a + d) - Cc]e'^2$$

und daher:

$$B(a + d) = 0.$$

Endlich wird aus $a \cdot [3] - b \cdot [2]$:

$$(Bb + Cd)(ad - bc) = (-Bb + Ca)e'^2$$

und daher:

$$C(a + d) = 0.$$

Da nun nicht alle drei Grössen A, B, C gleich Null sein können, wird notwendig $a + d = 0$ oder $a = -d$ sein.

Aus $a \cdot [2] - b \cdot [1]$ folgt:

$$(Ba + Cc)(ad - bc) = (Ba - Ab)e'^2,$$

somit:

$$[5] \qquad Ab - 2Ba - Cc = 0.$$

Aus den Gleichungen $e + e' = 0$, $a + d = 0$ oder

$$\alpha\delta - \beta\gamma + \alpha'\delta' - \beta'\gamma' = 0, \quad \alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha' = 0$$

folgt: $(\alpha + \alpha')(\delta + \delta') = (\beta + \beta')(\gamma + \gamma')$ oder:

$$(\alpha + \alpha') : (\gamma + \gamma') = (\beta + \beta') : (\delta + \delta').$$

Das Verhältnis, welches diesem Verhältnis*) in kleinsten Zahlen ausgedrückt gleich ist, sei $m : n$, so dass m und n prim zu einander sind, und man nehme μ, ν derart an, dass $\mu m + \nu n = 1$ ist. Ferner sei r der grösste gemeinschaftliche Teiler der Zahlen $a, b, c,$ dessen Quadrat somit auch in

*) Wenn alle Grössen $\alpha + \alpha'$, $\gamma + \gamma'$, $\beta + \beta'$, $\delta + \delta'$ gleich Null wären, würde das Verhältnis unbestimmt und daher die Methode nicht anwendbar sein. Aber geringe Aufmerksamkeit lehrt, dass dies mit unsern Annahmen nicht verträglich ist. Denn es würde sein: $\alpha\delta - \beta\gamma = \alpha'\delta' - \beta'\gamma'$ d. i. $e = e'$ und daher, weil $e = -e'$ ist, $e = e' = 0$. Hieraus würde auch $B'^2 - A'C'$ d. h. die Determinante der Form F' gleich Null werden, welche Formen wir ganz und gar ausgeschlossen haben.

a^2+bc oder $bc-ad$ oder e^2 aufgehen wird, so dass r auch ein Teiler von e ist. Hat man dies alles so gemacht und nimmt man an, dass die Form F durch die Substitution

$$x=mt+\frac{\nu e}{r}u,\quad y=nt-\frac{\mu e}{r}u$$

in die Form $Mt^2+2Ntu+Pu^2$ oder G übergeht, so wird diese ambig sein und die Form F' enthalten.

Beweis. I. Damit ersichtlich werde, dass die Form G ambig ist, werden wir zeigen, dass

$$M(b\mu^2-2a\mu\nu-c\nu^2)=2Nr$$

ist, wonach, da r in a, b, c aufgeht, $\frac{1}{r}(b\mu^2-2a\mu\nu-c\nu^2)$ eine ganze Zahl und somit $2N$ ein Vielfaches von M wird. Es ist aber:

[6] $M=Am^2+2Bmn+Cn^2,\quad Nr=[Am\nu-B(m\mu-n\nu)-Cn\mu]e.$

Ferner bestätigt man durch Entwicklung leicht, dass

$$2e+2a=e-e'+a-d=(\alpha-\alpha')(\delta+\delta')-(\beta-\beta')(\gamma+\gamma')$$
$$2b=(\alpha+\alpha')(\beta-\beta')-(\alpha-\alpha')(\beta+\beta')$$

ist. Hieraus folgt, da $m(\gamma+\gamma')=n(\alpha+\alpha')$, $m(\delta+\delta')=n(\beta+\beta')$ ist:

$$m(2e+2a)=-2nb\ \text{ oder:}$$

[7] $$me+ma+nb=0.$$

Auf analoge Weise ist:

$$2e-2a=e-e'-a+d=(\alpha+\alpha')(\delta-\delta')-(\beta+\beta')(\gamma-\gamma'),$$
$$2c=(\gamma-\gamma')(\delta+\delta')-(\gamma+\gamma')(\delta-\delta'),$$

und hieraus folgt $n(2e-2a)=-2mc$ oder:

[8] $$ne-na+mc=0.$$

Wenn man nun zu $m^2(b\mu^2-2a\mu\nu-c\nu^2)$ den Ausdruck

$$(1-m\mu-n\nu)[m\nu(e-a)+(m\mu+1)b]+(me+ma+nb)(m\mu\nu+\nu)$$
$$+(ne-na+mc)m\nu^2,$$

welcher wegen

$$1-m\mu-n\nu=0,\quad me+ma+nb=0,\quad ne-na+mc=0$$

offenbar gleich Null ist, addiert, so erhält man, nachdem man die Producte der Regel nach entwickelt und die sich aufhebenden Teile weggelassen hat, $2m\nu e+b$. Demnach ist:

[9] $$m^2(b\mu^2-2a\mu\nu-c\nu^2)=2m\nu e+b.$$

Addiert man in analoger Weise zu $mn(b\mu^2-2a\mu\nu-c\nu^2)$ den Ausdruck:

$$(1-m\mu-n\nu)[(n\nu-m\mu)e-(1+m\mu+n\nu)a]-(me+ma+nb)m\mu^2$$
$$+(ne-na+mc)n\nu^2,$$

so findet man:

[10] $$mn(b\mu^2 - 2a\mu\nu - c\nu^2) = (n\nu - m\mu)e - a.$$

Addiert man endlich zu $n^2(b\mu^2 - 2a\mu\nu - c\nu^2)$ den Ausdruck:

$$(m\mu + n\nu - 1)[n\mu(e+a) + (\nu n + 1)c] - (me + ma + nb)n\mu^2 - (ne - na + mc)(n\mu\nu + \mu),$$

so wird:

[11] $$n^2(b\mu^2 - 2a\mu\nu - c\nu^2) = -2n\mu e - c.$$

Aus [9], [10], [11] ergiebt sich nun:

$$(Am^2 + 2Bmn + Cn^2)(b\mu^2 - 2a\mu\nu - c\nu^2) = 2e[Am\nu + B(n\nu - m\mu) - Cn\mu] + Ab - 2Ba - Cc$$

oder wegen [6]:

$$M(b\mu^2 - 2a\mu\nu - c\nu^2) = 2Nr.$$

II. Um zu beweisen, dass die Form G die Form F' enthält, werden wir zeigen, erstens dass G in F' übergeht, wenn man setzt:

$$(S)\quad t = (\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y',\ u = \frac{r}{e}(n\alpha - m\gamma)x' + \frac{r}{e}(n\beta - m\delta)y',$$

zweitens dass $\frac{r}{e}(n\alpha - m\gamma)$ und $\frac{r}{e}(n\beta - m\delta)$ ganze Zahlen sind.

1. Da F in G übergeht, wenn man setzt:

$$x = mt + \frac{\nu e}{r}u,\ y = nt - \frac{\mu e}{r}u,$$

so wird G durch die Substitution (S) in dieselbe Form transformiert werden, in welche F transformiert wird, wenn man setzt:

$$\begin{aligned} x &= m[(\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y'] + \nu[(n\alpha - m\gamma)y' + (n\beta - m\delta)y'] \\ &= \alpha(m\mu + n\nu)x' + \beta(m\mu + n\nu)y' = \alpha x' + \beta y', \\ \text{und } y &= n[(\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y'] - \mu[(n\alpha - m\gamma)x' + (n\beta - m\delta)y'] \\ &= \gamma(n\nu + m\mu)x' + \delta(n\nu + m\mu)y' = \gamma x' + \delta y'. \end{aligned}$$

Durch diese Substitution geht aber F in F' über; daher wird durch die Substitution (S) auch G in F' übergehen.

2. Aus den Werten von e, b, d findet man $\alpha' e + \gamma b - \alpha d = 0$ oder wegen $d = -a$: $n\alpha' e + n\alpha a + n\gamma b = 0$. Hieraus nach [7]: $n\alpha' e + n\alpha a = m\gamma e + m\gamma a$ oder:

[12] $$(n\alpha - m\gamma)a = (m\gamma - n\alpha')e.$$

Ferner wird: $\alpha nb = -\alpha m(e + a)$, $\gamma mb = -m(\alpha' e + \alpha a)$ und daher:

[13] $$(n\alpha - m\gamma)b = (\alpha' - \alpha)me.$$

Endlich ist $\gamma' e - \gamma a + \alpha c = 0$; hieraus entsteht, wenn man mit n multipliciert und für $n\alpha$ seinen Wert aus [8] setzt:

[14] $$(n\alpha - m\gamma)c = (\gamma - \gamma')ne.$$

Auf analoge Weise leitet man ab: $\beta' e + \delta b - \beta d = 0$ oder $n\beta' e + n\delta b + n\beta a = 0$ und daher nach [7]: $n\beta' e + n\beta a = m\delta e + m\delta a$ oder:

[15] $$(n\beta - m\delta) a = (m\delta - n\beta') e.$$

Ferner wird: $\beta n b = -\beta m(e + a)$, $\delta m b = -m(\beta' e + \beta a)$ und daher:

[16] $$(n\beta - m\delta) b = (\beta' - \beta) m e.$$

Schliesslich ist $\delta' e - \delta a + \beta c = 0$; hieraus entsteht, wenn man mit n multipliciert und für na seinen Wert aus [8] setzt:

[17] $$(n\beta - m\delta) c = (\delta - \delta') n e.$$

Da nun der grösste gemeinschaftliche Teiler der Zahlen a, b, c gleich r ist, so lassen sich ganze Zahlen $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ so annehmen, dass

$$\mathfrak{A}a + \mathfrak{B}b + \mathfrak{C}c = r$$

ist. Ist dies geschehen, so folgt aus [12], [13], [14]; [15], [16], [17]:

$$\mathfrak{A}(m\gamma - n\alpha') + \mathfrak{B}(\alpha' - \alpha) m + \mathfrak{C}(\gamma - \gamma') n = \frac{r}{e}(n\alpha - m\gamma)$$

$$\mathfrak{A}(m\delta - n\beta') + \mathfrak{B}(\beta' - \beta) m + \mathfrak{C}(\delta - \delta') n = \frac{r}{e}(n\beta - m\delta);$$

mithin sind $\frac{r}{e}(n\alpha - m\gamma)$ und $\frac{r}{e}(n\beta - m\delta)$ ganze Zahlen.

165.

Beispiel. Die Form $3x^2 + 14xy - 4y^2$ wird transformiert in die Form $-12x'^2 - 18x'y' + 39y'^2$, sowohl eigentlich, wenn man setzt:

$$x = 4x' + 11y', \quad y = -x' - 2y',$$

als auch uneigentlich, wenn man setzt:

$$x = -74x' + 89y', \quad y = 15x' - 18y'.$$

Hier sind also die Zahlen $\alpha + \alpha'$, $\beta + \beta'$, $\gamma + \gamma'$, $\delta + \delta'$ bezüglich: -70, 100, 14, -20. Es ist aber $-70 : 14 = 100 : -20 = 5 : -1$. Wir setzen daher $m = 5$, $n = -1$, $\mu = 0$, $\nu = -1$. Als Zahlen a, b, c findet man -237, -1170, 48, deren grösster gemeinschaftlicher Teiler gleich $3 = r$ ist. Endlich wird $e = 3$. Hiernach wird die Transformation (S) die folgende: $x = 5t - u$, $y = -t$, und durch diese geht die Form $(3, 7, -4)$ über in die ambige Form $t^2 - 16tu + 3u^2$.

Sind die Formen F, F' äquivalent, so wird die Form G, wenn sie unter F enthalten ist, auch unter F' enthalten sein. Da sie aber dieselbe Form auch enthält, so wird sie derselben und folglich auch der Form F äquivalent sein. In diesem Falle lässt sich also der **Satz** so aussprechen:

Wenn die Formen F und F' sowohl eigentlich als auch uneigentlich äquivalent sind, so lässt sich eine beiden Formen äquivalente ambige Form finden.

Übrigens ist in diesem Falle $e = \pm 1$ und daher ist auch r, welches in e aufgeht, gleich 1.

Dies möge hinsichtlich der Transformation der Formen im Allgemeinen genügen; wir gehen daher zur Betrachtung der Darstellungen über.

Allgemeines über die Darstellungen von Zahlen durch Formen und deren Zusammenhang mit den Transformationen.

166.

Wenn die Form F die Form F' enthält, so lässt sich jede Zahl, welche durch F' dargestellt werden kann, auch durch F darstellen.

Es seien die Unbestimmten der Formen F, F' respective x, y; x', y', und man nehme an, dass die Zahl M durch F' dargestellt werde, wenn man $x' = m$, $y' = n$ setzt, die Form F aber in F' übergehe durch die Substitution:

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'.$$

Dann wird offenbar, wenn man

$$x = \alpha m + \beta n, \quad y = \gamma m + \delta n$$

setzt, F in M übergehen.

Wenn M sich auf mehrere Arten durch die Form F' darstellen lässt, z. B. auch wenn man $x' = m'$, $y' = n'$ setzt, so werden sich daraus auch mehrere Darstellungen von M durch F ergeben. Denn wenn sowohl $\alpha m + \beta n = \alpha m' + \beta n'$ als auch $\gamma m + \delta n = \gamma m' + \delta n'$ wäre, so würde entweder $\alpha\delta - \beta\gamma = 0$ und daher im Widerspruch mit unsrer Voraussetzung die Determinante der Form F gleich Null oder $m = m'$, $n = n'$ sein. Hieraus folgt, dass M mindestens auf ebenso viele verschiedene Arten durch F sich darstellen lässt wie durch F'.

Wenn daher sowohl F die Form F' als auch F' die Form F enthält, d. h. wenn F, F' äquivalent sind, und die Zahl M durch eine von beiden sich darstellen lässt, so lässt sie sich auch durch die andere darstellen und zwar durch die eine auf ebenso viele verschiedene Arten wie durch die andere.

Schliesslich bemerken wir, dass in diesem Falle der grösste gemeinschaftliche Teiler der Zahlen m, n gleich ist dem grössten gemeinschaftlichen Teiler der Zahlen $\alpha m + \beta n$, $\gamma m + \delta n$. Ist jener gleich Δ und sind die Zahlen μ, ν derart angenommen, dass $\mu m + \nu n = \Delta$ ist, so wird:

$$(\delta\mu - \gamma\nu)(\alpha m + \beta n) - (\beta\mu - \alpha\nu)(\gamma m + \delta n) = (\alpha\delta - \beta\gamma)(\mu m + \nu n) = \pm \Delta.$$

Hiernach geht der grösste gemeinschaftliche Teiler der Zahlen $\alpha m + \beta n$, $\gamma m + \delta n$ auch in Δ, Δ aber wiederum auch in jenem auf, weil es offenbar in $\alpha m + \beta n$ und $\gamma m + \delta n$ aufgeht. Somit muss jener notwendig gleich Δ

sein. — Wenn also m, n zu einander prim sind, werden auch $\alpha m + \beta n$, $\gamma m + \delta n$ zu einander prim sein.

167.

Satz. Wenn die Formen

$$ax^2 + 2bxy + cy^2 \text{ oder } F,$$
$$a'x'^2 + 2b'x'y' + c'y'^2 \text{ oder } F'$$

äquivalent sind, ihre Determinante gleich D ist und die letztere in die erstere übergeht, wenn man setzt:

$$x' = \alpha x + \beta y, \quad y' = \gamma x + \delta y,$$

wenn ferner die Zahl M durch F dargestellt wird, wenn man $x = m$, $y = n$ macht, und daher durch F', wenn man

$$x' = \alpha m + \beta n = m', \quad y' = \gamma m + \delta n = n'$$

setzt, und zwar so, dass m zu n und demnach auch m' zu n' prim ist, so werden beide Darstellungen entweder zu demselben Werte oder zu entgegengesetzten Werten des Ausdrucks $\sqrt{D}$ (mod. M) gehören, je nachdem die Transformation der Form F' in F eine eigentliche oder uneigentliche ist.

Beweis. Man bestimme die Zahlen μ, ν derart, dass $\mu m + \nu n = 1$ ist und setze:

$$\frac{\delta\mu - \gamma\nu}{\alpha\delta - \beta\gamma} = \mu', \qquad \frac{-\beta\mu + \alpha\nu}{\alpha\delta - \beta\gamma} = \nu'$$

(welche Grössen wegen $\alpha\delta - \beta\gamma = \pm 1$ ganze Zahlen sind), so wird (nach dem Ende des vorigen Artikels):

$$\mu' m' + \nu' n' = 1.$$

Ist ferner

$$\mu(bm + cn) - \nu(am + bn) = V, \quad \mu'(b'm' + c'n') - \nu'(a'm' + b'n') = V',$$

so werden V, V' Werte des Ausdrucks $\sqrt{D}$ (mod. M) sein, zu welchen die erste und zweite Darstellung gehören. Werden in V' für μ', ν', m', n' ihre Werte, in V aber

für a: $a'\alpha^2 + 2b'\alpha\gamma + c'\gamma^2$
für b: $a'\alpha\beta + b'(\alpha\delta + \beta\gamma) + c'\gamma\delta$
für c: $a'\beta^2 + 2b'\beta\delta + c'\delta^2$

gesetzt, so findet man nach Ausführung der Entwicklung:

$$V = V'(\alpha\delta - \beta\gamma).$$

Demnach ist entweder $V = V'$ oder $V = -V'$, je nachdem $\alpha\delta - \beta\gamma = +1$ oder $= -1$ ist, d. h. die Darstellungen werden zu einem und demselben

oder zu entgegengesetzten Werten des Ausdrucks $\sqrt{D}$ (mod. M) gehören, je nachdem die Transformation der Form F' in F eine eigentliche oder eine uneigentliche ist.

Wenn man daher vermittelst einander primer Werte der Unbestimmten x, y mehrere Darstellungen der Zahl M durch die Form (a, b, c) hat, welche zu verschiedenen Werten des Ausdrucks $\sqrt{D}$ (mod. M) gehören, so werden die entsprechenden Darstellungen durch die Form (a', b', c') bezüglich zu denselben Werten gehören, und wenn es keine Darstellung der Zahl M durch irgend eine Form giebt, welche zu irgend einem bestimmten Werte gehört, so wird es auch keine zu diesem Werte gehörige Darstellung durch die zu jener äquivalente Form geben.

168.

Satz. Wenn die Zahl M durch die Form $ax^2 + 2bxy + cy^2$ dargestellt wird, wenn man den Unbestimmten x, y die zu einander primen Werte m, n beilegt, und wenn der Wert des Ausdrucks $\sqrt{D}$ (mod. M), zu welchem diese Darstellung gehört, gleich N ist, so werden die Formen (a, b, c) und $\left(M, N, \frac{N^2 - D}{M}\right)$ eigentlich äquivalent sein.

Beweis. Aus Artikel 155 geht hervor, dass sich ganze Zahlen μ, ν von der Beschaffenheit finden lassen, dass

$$m\mu + n\nu = 1, \quad \mu(bm + cn) - \nu(am + bn) = N$$

ist. Ist dies geschehen, so geht die Form (a, b, c) durch die Substitution $x = mx' - \nu y'$, $y = nx' + \mu y'$, welche offenbar eine eigentliche ist, in eine Form, deren Determinante gleich $D(m\mu + n\nu)^2$ d. h. gleich D ist, oder in eine äquivalente Form über. Setzt man diese Form gleich $\left(M', N', \frac{N'^2 - D}{M'}\right)$, so wird:

$$M' = am^2 + 2bmn + cn^2 = M, \quad N' = -m\nu a + (m\mu - n\nu)b + n\mu c = N.$$

Daher wird die Form, in welche (a, b, c) durch jene Transformation verwandelt wird, dargestellt durch $\left(M, N, \frac{N^2 - D}{M}\right)$.

Aus den Gleichungen

$$m\mu + n\nu = 1, \quad \mu(mb + nc) - \nu(ma + nb) = N$$

folgt übrigens:

$$\mu = \frac{nN + ma + nb}{am^2 + 2bmn + cn^2} = \frac{nN + ma + nb}{M}, \quad \nu = \frac{mb + nc - mN}{M},$$

welche Zahlen somit ganze Zahlen sind.

Ferner ist zu bemerken, dass dieser Satz nicht gilt, wenn $M=0$ ist, denn dann wird das Glied $\frac{N^2-D}{M}$ unbestimmt.*)

169.

Wenn man mehrere Darstellungen der Zahl M durch (a, b, c) hat, welche zu demselben Werte N des Ausdrucks $\sqrt{D}\,(\text{mod.}\,M)$ gehören (wobei wir immer die Werte von x, y zu einander prim voraussetzen), so lassen sich daraus auch mehrere eigentliche Transformationen der Form (a, b, c) oder F in die Form $\left(M, N, \frac{N^2-D}{M}\right)$ oder G ableiten. Wenn nämlich auch aus den Werten $x=m'$, $y=n'$ eine solche Darstellung hervorgeht, so wird F auch durch die Substitution

$$x=m'x'+\frac{m'N-m'b-n'c}{M}y',\quad y=n'x'+\frac{n'N+m'a+n'b}{M}y'$$

in G übergehen. Umgekehrt wird sich aus jeder eigentlichen Transformation der Form F in G eine Darstellung der Zahl M durch die Form F, welche zum Werte N gehört, ergeben. Wenn nämlich F in G übergeht dadurch, dass man setzt: $x=mx'-\nu y'$, $y=nx'+\mu y'$, so wird M dargestellt durch F, wenn $x=m$, $y=n$ gesetzt wird, und da hier $m\mu+n\nu=1$ ist, so wird der Wert des Ausdrucks $\sqrt{D}\,(\text{mod.}\,M)$, zu welchem die Darstellung gehört, gleich $\mu(bm+cn)-\nu(am+bn)$ d. i. N sein. Aus mehreren verschiedenen eigentlichen Transformationen aber werden ebenso viele verschiedene zu N gehörende Darstellungen sich ergeben.**) — Hieraus folgt leicht, dass, wenn man alle eigentlichen Transformationen der Form F in G hat, aus diesen sämtliche zum Werte N gehörende Darstellungen von M durch F folgen. Somit ist die Aufgabe, die Darstellungen einer gegebenen Zahl durch eine gegebene Form zu ermitteln (in denen die Unbestimmten zu einander prime Werte erhalten), zurückgeführt auf die Aufgabe, alle eigentlichen Transformationen jener Form in eine gegebene äquivalente Form zu finden.

---

*) Wenn wir unsere Ausdrucksweise auch auf diesen Fall anwenden wollen, so wird die Redensart: N sei ein Wert des Ausdrucks $\sqrt{D}\,(\text{mod.}\,M)$ oder es sei $N^2\equiv D\,(\text{mod.}\,M)$, bedeuten, dass N^2-D ein Vielfaches von M und daher $=0$ sei.

**) Wenn man annimmt, dass aus zwei verschiedenen eigentlichen Transformationen dieselbe Darstellung hervorgehe, so werden jene sich folgendermassen verhalten müssen:

$$1.\quad x=mx'-\nu y',\quad y=nx'+\mu y',\qquad 2.\quad x=mx'-\nu'y',\quad y=nx'+\mu'y'.$$

Aus den beiden Gleichungen

$$m\mu+n\nu=m\mu'+n\nu',\quad \mu(mb+nc)-\nu(ma+nb)=\mu'(mb+nc)-\nu'(ma+nb)$$

folgt aber leicht, dass entweder $M=0$ oder $\mu=\mu'$, $\nu=\nu'$ ist. Der Fall $M=0$ ist jedoch ausgeschlossen.

Wendet man nun hierauf das an, was wir im Artikel 162 dargelegt haben, so ergiebt sich leicht, dass, wenn irgend eine zum Werte N gehörende Darstellung der Zahl M durch die Form F die folgende ist: $x = \alpha$, $y = \gamma$, alsdann die allgemeine Formel, welche alle zum Werte N gehörenden Darstellungen derselben Zahl durch die Form F umfasst, die folgende ist:

$$x = \frac{\alpha t - (\alpha b + \gamma c)u}{m}, \quad y = \frac{\gamma t + (\alpha a + \gamma b)u}{m},$$

wo m der grösste gemeinschaftliche Teiler der Zahlen a, $2b$, c ist und t, u unbestimmt alle Zahlen bedeuten, welche der Gleichung $t^2 - Du^2 = m^2$ genügen.

170.

Wenn die Form (a, b, c) irgend einer ambigen Form äquivalent ist, also der Form $\left(M, N, \frac{N^2 - D}{M}\right)$ sowohl eigentlich als auch uneigentlich oder sowohl der Form $\left(M, N, \frac{N^2 - D}{M}\right)$ als auch der Form $\left(M, -N, \frac{N^2 - D}{M}\right)$ eigentlich äquivalent ist, so erhält man mittelst der Form F die Darstellungen der Zahl M, welche sowohl zum Werte N als auch zum Werte $-N$ gehören. Und umgekehrt, wenn man mehrere Darstellungen der Zahl M durch dieselbe Form F hat, welche zu entgegengesetzten Werten N und $-N$ des Ausdrucks $\sqrt{D}$ (mod. M) gehören, so ist die Form F der Form G sowohl eigentlich als auch uneigentlich äquivalent, und es kann eine ambige Form gefunden werden, welcher F äquivalent ist.

Diese allgemeinen Bemerkungen über die Darstellungen mögen an dieser Stelle genügen: Über die Darstellungen, in welchen die Unbestimmten zu einander nicht prime Werte haben, werden wir weiter unten sprechen. In Bezug auf andere Eigenschaften müssen die Formen mit negativer Determinante auf ganz andere Weise behandelt werden als diejenigen mit positiver Determinante. Daher werden wir sie von nun an gesondert betrachten und beginnen mit jenen als den leichteren.

Über die Formen mit negativer Determinante.

171.

Aufgabe. Wenn irgend eine Form (a, b, a'), deren Determinante negativ und gleich $-D$ ist, wo D eine positive Zahl bezeichnet, gegeben ist, so soll man eine dieser eigentlich äquivalente Form (A, B, C) finden, in welcher A weder grösser als $\sqrt{\frac{4}{3}D}$ und C, noch kleiner als $2B$ ist.

Auflösung. Wir nehmen an, dass in der gegebenen Form nicht alle drei Bedingungen gleichzeitig erfüllt sind, denn sonst brauchte man keine andere Form zu suchen. Es sei b' der absolut kleinste Rest der Zahl $-b$

nach dem Modul a'*) und $a''=\frac{b'^2+D}{a'}$, welches eine ganze Zahl ist, weil $b'^2\equiv b^2$, $b'^2+D\equiv b^2+D\equiv aa'\equiv 0 \pmod{a'}$ ist. Ist nun $a''<a'$, so sei wiederum b'' der absolut kleinste Rest von $-b'$ nach dem Modul a'' und $a'''=\frac{b''^2+D}{a''}$. Ist auch hier noch $a'''<a''$, so sei wiederum b''' der absolut kleinste Rest von $-b''$ nach dem Modul a''' und $a''''=\frac{b'''^2+D}{a'''}$. Diese Operation setze man fort, bis man in der Reihe $a', a'', a''', a'''', \ldots$ zu einem Gliede $a^{(m+1)}$ gelangt, welches nicht kleiner ist als das ihm vorhergehende $a^{(m)}$; dieses muss schliesslich einmal eintreten, weil man sonst eine unendliche Reihe fortwährend abnehmender ganzer Zahlen haben würde. Dann wird die Form $(a^{(m)}, b^{(m)}, a^{(m+1)})$ allen Bedingungen genügen.

Beweis. I. In der Reihe der Formen (a, b, a'), (a', b', a''), (a'', b'', a'''), ... ist jede der vorhergehenden benachbart, daher ist die letzte der ersten eigentlich äquivalent (Artikel 159, 160).

II. Da $b^{(m)}$ der absolut kleinste Rest von $-b^{(m-1)}$ nach dem Modul $a^{(m)}$ ist, so kann er nicht grösser als $\frac{1}{2}a^{(m)}$ sein (Artikel 4).

III. Da $a^{(m)}a^{(m+1)}=D+b^{(m)2}$ und $a^{(m+1)}$ nicht kleiner als $a^{(m)}$ ist, so wird $a^{(m)2}$ nicht grösser als $D+b^{(m)2}$ sein, und da $b^{(m)}$ nicht grösser als $\frac{1}{2}a^{(m)}$ ist, so wird $a^{(m)2}$ nicht grösser als $D+\frac{1}{4}a^{(m)2}$, also $\frac{3}{4}a^{(m)2}$ nicht grösser als D und schliesslich $a^{(m)}$ nicht grösser als $\sqrt{\frac{4}{3}D}$ sein.

Beispiel. Die gegebene Form sei (304, 217, 155), deren Determinante gleich -31 ist. Hier findet man die Reihe der Formen:

(304, 217, 155), (155, -62, 25), (25, 12, 7), (7, 2, 5), (5, -2, 7).

Die letzte ist die gesuchte. — In derselben Weise findet man für die Form (121, 49, 20), deren Determinante gleich -19 ist, die äquivalenten Formen: (20, -9, 5), (5, -1, 4), (4, 1, 5); somit ist (4, 1, 5) die gesuchte Form.

Derartige Formen (A, B, C), deren Determinante negativ und in denen A weder grösser als $\sqrt{\frac{4}{3}D}$ und C, noch kleiner als $2B$ ist, werden wir **reducierte Formen** nennen. Somit kann zu jeder Form mit negativer Determinante eine eigentlich äquivalente reducierte Form gefunden werden.

172.

Aufgabe. Die Bedingungen zu finden, unter denen zwei nicht identische reducierte Formen mit derselben Determinante $-D$, (a, b, c) und (a', b', c'), eigentlich äquivalent sein können.

---

*) Man bemerke, dass, wenn das erste oder letzte Glied a oder a' einer Form (a, b, a') gleich 0 ist, die Determinante derselben ein positives Quadrat ist; somit kann jenes im vorliegenden Falle nicht stattfinden. — Aus ähnlichem Grunde können die äusseren Glieder a, a' einer Form mit negativer Determinante nicht entgegengesetzte Zeichen haben.

Auflösung. Nehmen wir, was erlaubt ist, an, dass a' nicht grösser als a sei und dass die Form $ax^2 + 2bxy + cy^2$ in die Form $a'x'^2 + 2b'x'y' + c'y'^2$ durch die eigentliche Substitution $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ übergehe, so haben wir die Gleichungen:

$$[1] \qquad a\alpha^2 + 2b\alpha\gamma + c\gamma^2 = a'$$
$$[2] \qquad a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b'$$
$$[3] \qquad \alpha\delta - \beta\gamma = 1.$$

Aus [1] folgt $aa' = (a\alpha + b\gamma)^2 + D\gamma^2$, somit ist aa' positiv, und da $ac = D + b^2$, $a'c' = D + b'^2$ ist, so sind auch ac oder $a'c'$ positiv. Demnach haben alle Zahlen a, a', c, c' dasselbe Vorzeichen. Da nun sowohl a als auch a' nicht grösser als $\sqrt{\frac{4}{3}D}$ ist, so ist aa' nicht grösser als $\frac{4}{3}D$ und somit kann um so weniger $D\gamma^2$ (welches gleich $aa' - (a\alpha + b\gamma)^2$ ist) grösser als $\frac{4}{3}D$ sein. Hiernach ist γ entweder gleich Null oder gleich ± 1.

I. Ist $\gamma = 0$, so folgt aus [3], dass entweder $\alpha = 1$, $\delta = 1$ oder $\alpha = -1$, $\delta = -1$ ist. In beiden Fällen wird aus [1]: $a' = a$ und aus [2]: $b' - b = \pm \beta a$. Nun ist aber b nicht grösser als $\frac{1}{2}a$ und b' nicht grösser als $\frac{1}{2}a'$ und somit auch nicht grösser als $\frac{1}{2}a$. Demnach kann die Gleichung $b' - b = \pm \beta a$ nur dann bestehen, wenn

entweder $b = b'$ ist; dann würde hieraus $c' = \dfrac{b'^2 + D}{a'} = \dfrac{b^2 + D}{a} = c$ folgen, es würden mithin im Widerspruch mit der Voraussetzung die Formen (a, b, c) und (a', b', c') identisch sein.

oder $b = -b' = \pm \frac{1}{2}a$ ist; in diesem Falle ist $c' = c$ und die Form (a', b', c') geht in $(a, -b, c)$ d. i. in die der Form (a, b, c) entgegengesetzte über. Zugleich erhellt, dass diese Formen ambig sind, da $2b = \pm a$ ist.

II. Ist $\gamma = \pm 1$, so wird aus [1]: $a\alpha^2 + c - a' = \pm 2b\alpha$. Da aber c nicht kleiner als a und daher nicht kleiner als a' ist, so ist $a\alpha^2 + c - a'$ oder $2b\alpha$ sicher nicht kleiner als $a\alpha^2$. Somit wird, da $2b$ nicht grösser ist als a, α nicht kleiner als α^2; und hieraus folgt notwendig $\alpha = 0$ oder $\alpha = \pm 1$.

1. Ist $\alpha = 0$, so wird aus [1] $a' = c$, und da a weder grösser als c noch kleiner als a' ist, so wird notwendig $a' = a = c$. Weiter wird aus [3]: $\beta\gamma = -1$ und somit aus [2]: $b + b' = \pm \delta c = \pm \delta a$. Hieraus folgt in ähnlicher Weise wie in I, dass

entweder $b = b'$ ist, in welchem Falle die Formen (a, b, c), (a', b', c') gegen die Voraussetzung identisch sein würden,

oder $b = -b'$ ist, in welchem Falle die Formen (a, b, c), (a', b', c') entgegengesetzt sind.

2. Ist $\alpha = \pm 1$, so folgt aus [1]: $\pm 2b = a + c - a'$, und da weder a noch c kleiner als a' ist, so wird $2b$ nicht kleiner als a und nicht kleiner als c sein. Es ist aber auch $2b$ nicht grösser als a und nicht grösser als

c; daher ist notwendig $\pm 2b = a = c$ und somit infolge der Gleichung $\pm 2b = a + c - a'$ auch gleich a'. Es wird also aus [2]

$$b' = a(\alpha\beta + \gamma\delta) + b(\alpha\delta + \beta\gamma)$$

oder wegen $\alpha\delta - \beta\gamma = 1$:

$$b' - b = a(\alpha\beta + \gamma\delta) + 2b\beta\gamma = a(\alpha\beta + \gamma\delta \pm \beta\gamma),$$

daher notwendig wie vorher

entweder $b = b'$, wonach die Formen (a, b, c), (a', b', c') gegen die Voraussetzung identisch sein würden;

oder $b = -b'$, wo dann jene Formen entgegengesetzt sind. Gleichzeitig sind in diesem Falle wegen $a = \pm 2b$ die Formen ambig.

Aus allem diesem folgt, dass die Formen (a, b, c) und $(a'\ b'\ c')$ nur dann eigentlich äquivalent sein können, wenn sie entgegengesetzt sind und gleichzeitig entweder ambig sind oder $a = c = a' = c'$ ist. Dass in diesen Fällen die Formen (a, b, c) und (a', b', c') eigentlich äquivalent sind, hätte man auch von vornherein leicht sehen könnnn. Denn wenn die Formen entgegengesetzt sind, müssen sie uneigentlich, und, wenn sie überdies ambig sind, auch eigentlich äquivalent sein. Ist aber $a = c$, so wird die Form $\left(\frac{D + (a-b)^2}{a}, a - b, a\right)$ der Form (a, b, c) benachbart und somit äquivalent sein. Wegen $D + b^2 = ac = a^2$ ist aber $\frac{D + (a-b)^2}{a} = 2a - 2b$ und die Form $(2a - 2b, a - b, a)$ ist ambig. Mithin wird die Form (a, b, c) der zu ihr entgegengesetzten auch eigentlich äquivalent sein.

Ebenso leicht kann man nun entscheiden, wann zwei nicht entgegengesetzte reducierte Formen (a, b, c) und (a', b', c') uneigentlich äquivalent sein können. Sie werden nämlich uneigentlich äquivalent sein, wenn (a, b, c) und $(a', -b', c')$, welche nicht identisch sein werden, eigentlich äquivalent sind, und umgekehrt. Hieraus geht hervor, dass die Bedingung, unter welcher jene uneigentlich äquivalent sind, die ist, dass sie identisch sind und überdies entweder ambig sind oder $a = c$ ist. — Reducierte Formen aber, welche weder identisch noch entgegengesetzt sind, können weder eigentlich noch uneigentlich äquivalent sein.

173.

Aufgabe. Wenn zwei Formen F und F' mit derselben negativen Determinante gegeben sind, so soll man ermitteln, ob sie äquivalent sind.

Auflösung. Man suche die beiden reducierten Formen f, f', welche den Formen F, F' respective eigentlich äquivalent sind. Wenn dann die Formen f, f' eigentlich oder uneigentlich oder auf beiderlei Weise äquivalent sind, werden es auch F, F' sein. Wenn aber f, f' auf keinerlei Weise äquivalent sind, werden es auch F, F' nicht sein.

Dem vorigen Artikel zufolge kann es vier Fälle geben:

1. Wenn f, f' weder identisch noch entgegengesetzt sind, so können F, F' auf keine Weise äquivalent sein.

2. Wenn f, f' erstens entweder identisch oder entgegengesetzt sind und zweitens entweder ambig sind oder je gleiche äussere Glieder haben, so werden F, F' sowohl eigentlich als uneigentlich äquivalent sein.

3. Wenn f, f' identisch, aber nicht ambig sind und auch keine gleichen äusseren Glieder haben, so werden F, F' nur eigentlich äquivalent sein.

4. Wenn f, f' entgegengesetzt, aber weder ambig sind noch auch gleiche äussere Glieder haben, so werden F, F' nur uneigentlich äquivalent sein.

Beispiel. Für die Formen (41, 35, 30), (7, 18, 47), deren Determinante gleich -5 ist, erweisen sich die reducierten Formen (1, 0, 5), (2, 1, 3) als nicht äquivalent. Daher sind jene in keiner Weise äquivalent. — Den Formen (23, 38, 63), (15, 20, 27) aber ist dieselbe reducierte Form (2, 1, 3) äquivalent und, da diese gleichzeitig ambig ist, so werden die Formen (23, 38, 63), (15, 20, 27) sowohl eigentlich als uneigentlich äquivalent sein. — Den Formen (37, 53, 78) und (53, 73, 102) sind die reducierten Formen (9, 2, 9), (9, -2, 9) äquivalent, und da diese entgegengesetzt und ihre äusseren Glieder gleich sind, so werden die gegebenen Formen sowohl eigentlich als auch uneigentlich äquivalent sein.

174.

Die Anzahl aller reducierten Formen, welche eine gegebene Determinante $-D$ haben, ist stets endlich und im Verhältnis zur Zahl D nur mässig gross. Diese Formen selbst aber können auf doppelte Weise gefunden werden. Wir wollen die reducierten Formen der Determinante $-D$ unbestimmt mit (a, b, c) bezeichnen, wo somit alle Werte von a, b, c bestimmt werden sollen.

Erste Methode. Man nehme für a alle Zahlen, sowohl positive als auch negative, welche nicht grösser als $\sqrt{\frac{4}{3}D}$ sind und von denen $-D$ quadratischer Rest ist, und für die einzelnen a setze man b der Reihe nach gleich allen sowohl positiv wie negativ genommenen Werten des Ausdrucks $\sqrt{-D}$ (mod. a), welche nicht grösser als $\frac{1}{2}a$ sind; c aber werde für die einzelnen bestimmten Werte von a, b gleich $\dfrac{D+b^2}{a}$ gesetzt. Wenn auf diese Weise irgend welche Formen entstehen, in denen $c < a$ ist, so sind diese zu verwerfen; die übrigen werden aber offenbar reduciert sein.

Zweite Methode. Man nehme für b alle Zahlen, sowohl positive wie negative, welche nicht grösser als $\frac{1}{2}\sqrt{\frac{4}{3}D}$ oder $\sqrt{\frac{1}{3}D}$ sind, zerlege für die einzelnen b den Ausdruck $b^2 + D$ auf alle nur möglichen Weisen (auch mit Berücksichtigung der Verschiedenheit der Vorzeichen) in je zwei Factoren,

die beide nicht grösser als $2b$ sind, und setze den einen Factor, und zwar, wenn die Factoren ungleich sind, den kleineren gleich a, den andern gleich c. Da a nicht grösser als $\sqrt{\frac{4}{3}D}$ ist, so werden offenbar alle auf diese Weise sich ergebenden Formen reducierte sein. — Schliesslich ist klar, dass es keine reducierte Form geben kann, die nicht durch jede der beiden Methoden gefunden würde.

Beispiel. Es sei $D = 85$. Hier ist die Grenze der Werte von a gleich $\sqrt{\frac{340}{3}}$, welche zwischen 10 und 11 liegt. Die Zahlen aber zwischen 1 und 10 (einschliesslich), deren Rest -85 ist, sind: 1, 2, 5, 10. Hieraus erhält man die zwölf Formen:

$$(1, 0, 85), (2, 1, 43), (2, -1, 43), (5, 0, 17), (10, 5, 11), (10, -5, 11); (-1, 0, -85), (-2, 1, -43), (-2, -1, -43), (-5, 0, -17), (-10, 5, -11), (-10, -5, -11).$$

Nach der andern Methode erhält man als Grenze für die Werte von b die Zahl $\sqrt{\frac{85}{3}}$, welche zwischen 5 und 6 liegt. Für $b = 0$ entstehen die Formen: (1, 0, 85), (−1, 0, −85), (5, 0, 17), (−5, 0, −17); für $b = \pm 1$ die folgenden: (2, ±1, 43), (−2, ±1, −43). Für $b = \pm 2$ erhält man keine, da sich 89 nicht in zwei Factoren, die beide nicht kleiner als 4 sind, zerlegen lässt. Dasselbe gilt von ±3, ±4. Schliesslich entstehen aus $b = \pm 5$ die folgenden Formen: (10, ±5, 11), (−10, ±5, −11).

175.

Wenn man aus allen reducierten Formen einer gegebenen Determinante von je zwei Formen, welche, wenn auch nicht identisch, doch eigentlich äquivalent sind, die eine oder die andere weglässt, so besitzen die übrig bleibenden Formen die ausgezeichnete Eigenschaft, dass jede beliebige Form mit derselben Determinante irgend einer von ihnen eigentlich äquivalent ist und zwar nur einer einzigen (denn sonst würden unter ihnen einige eigentlich äquivalent sein). Hieraus geht hervor, dass alle Formen mit derselben Determinante in ebenso viele Klassen verteilt werden können, als Formen übriggeblieben sind, indem man nämlich die derselben reducierten Form eigentlich äquivalenten Formen zu derselben Klasse rechnet. So bleiben z. B. für $D = 85$ die Formen:

$$(1, 0, 85), (2, 1, 43), (5, 0, 17), (10, 5, 11),$$
$$(-1, 0, -85), (-2, 1, -43), (-5, 0, -17), (-10, 5, -11),$$

so dass also alle Formen mit der Determinante -85 in acht Klassen verteilt werden können, je nachdem sie der ersten, zweiten, u. s. w. Form äquivalent sind. Es ist aber ersichtlich, dass die in dieselbe Klasse gesetzten Formen eigentlich äquivalent sind, dass dagegen Formen aus verschiedenen Klassen nicht eigentlich äquivalent sein können. Doch werden wir diesen Gegenstand der Klassifikation der Formen unten weit ausführlicher behandeln.

Hier fügen wir nur eine einzige Bemerkung hinzu. Schon oben haben wir gezeigt, dass, wenn die Determinante einer Form (a, b, c) negativ, gleich $-D$, ist, a und c dasselbe Zeichen haben (weil nämlich $ac = b^2 + D$ und somit positiv ist). Aus demselben Grunde erkennt man leicht, dass, wenn die Formen (a, b, c), (a', b', c') äquivalent sind, alle Grössen a, c, a', c' dasselbe Zeichen haben werden. Denn wenn die erstere in die letztere durch die Substitution $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ übergeht, so ist $a\alpha^2 + 2b\alpha\gamma + c\gamma^2 = a'$ und hieraus $aa' = (a\alpha + b\gamma)^2 + D\gamma^2$ und somit sicher nicht negativ. Da aber weder a noch a' gleich Null sein kann, so wird aa' positiv sein und mithin werden die Zeichen von a, a' dieselben sein.

Hiernach ist klar, dass die Formen, deren äussere Glieder positiv sind, von denen, deren äussere Glieder negativ sind, vollständig separiert sind, und es reicht hin, von den reducierten Formen nur diejenigen zu betrachten, welche positive äussere Glieder haben, da die übrigen in gleicher Anzahl vorhanden sind und aus jenen entstehen, wenn man den äusseren Gliedern entgegengesetzte Zeichen giebt; und eben dasselbe gilt von den Formen, welche von den reducierten wegzulassen und beizubehalten sind.

176.

Man sieht hier für gewisse negative Determinanten eine Tafel der Formen, nach denen alle übrigen Formen mit derselben Determinante in Klassen geschieden werden können. Den Bemerkungen im vorigen Artikel gemäss setzen wir aber nur die Hälfte her, nämlich diejenigen, deren äussere Glieder positiv sind.

D	
1	(1, 0, 1)
2	(1, 0, 2)
3	(1, 0, 3), (2, 1, 2)
4	(1, 0, 4), (2, 0, 2)
5	(1, 0, 5), (2, 1, 3)
6	(1, 0, 6), (2, 0, 3)
7	(1, 0, 7), (2, 1, 4)
8	(1, 0, 8), (2, 0, 4), (3, 1, 3)
9	(1, 0, 9), (2, 1, 5), (3, 0, 3)
10	(1, 0, 10), (2, 0, 5)
11	(1, 0, 11), (2, 1, 6), (3, 1, 4), (3, −1, 4)
12	(1, 0, 12), (2, 0, 6), (3, 0, 4), (4, 2, 4).

Es würde überflüssig sein, diese Tafel hier weiter fortzusetzen, da wir unten eine viel zweckmässigere Einrichtung derselben zeigen werden.

Offenbar also wird jede Form mit der Determinante -1 der Form $x^2 + y^2$, wenn die äusseren Glieder derselben positiv sind, dagegen der Form $-x^2 - y^2$, wenn sie negativ sind, eigentlich äquivalent sein. Jede

Form ferner mit der Determinante -2, deren äussere Glieder positiv sind, wird der Form x^2+2y^2, ebenso jede Form mit der Determinante -11, deren äussere Glieder positiv sind, irgend einer der Formen x^2+11y^2, $2x^2+2xy+6y^2$, $3x^2+2xy+4y^2$, $3x^2-2xy+4y^2$ eigentlich äquivalent sein.

177.

Aufgabe. Man hat eine Reihe von Formen, von denen jede der vorhergehenden nach rechts hin benachbart ist; gesucht wird irgend eine eigentliche Transformation der ersten in eine beliebige Form der Reihe.

Auflösung. Die gegebenen Formen seien:

$$(a,b,a')=F,\ (a',b',a'')=F',\ (a'',b'',a''')=F'',\ (a''',b''',a'''')=F''',\ \ldots$$

Die Grössen $\frac{b+b'}{a'}, \frac{b'+b''}{a''}, \frac{b''+b'''}{a'''}, \ldots$ mögen bezüglich mit $h', h'', h''', \ldots$ bezeichnet werden, und die Unbestimmten der Formen $F, F', F'', \ldots$ seien respective $x, y;\ x', y';\ x'', y'';\ \ldots$ Ferner nehme man an, dass F übergehe

in F', wenn man setzt: $x=\alpha' x'+\beta' y',\quad y=\gamma' x'+\delta' y'$
in F'', „ „ „ : $x=\alpha'' x''+\beta'' y'',\quad y=\gamma'' x''+\delta'' y''$
in F''', „ „ „ : $x=\alpha''' x'''+\beta''' y''',\quad y=\gamma''' x'''+\delta''' y'''$
u. s. w.

Dann leitet man, weil

F in F' übergeht, wenn man setzt: $x=-y',\quad y=x'+h' y'$
F' in F'' „ „ „ „ : $x'=-y'',\quad y'=x''+h'' y''$
F'' in F''' „ „ „ „ : $x''=-y''',\quad y''=x'''+h''' y'''$
u. s. w. (Artikel 160),

leicht folgenden Algorithmus her (Artikel 159):

$$\begin{array}{llll}
\alpha'=0, & \beta'=-1, & \gamma'=1, & \delta'=h' \\
\alpha''=\beta', & \beta''=h''\beta'-\alpha', & \gamma''=\delta', & \delta''=h''\delta'-\gamma' \\
\alpha'''=\beta'', & \beta'''=h'''\beta''-\alpha'', & \gamma'''=\delta'', & \delta'''=h'''\delta''-\gamma'' \\
\alpha''''=\beta''', & \beta''''=h''''\beta'''-\alpha''', & \gamma''''=\delta''', & \delta''''=h''''\delta'''-\gamma'''
\end{array}$$
u. s. w.,

oder:

$$\begin{array}{llll}
\alpha'=0, & \beta'=-1, & \gamma'=1, & \delta'=h' \\
\alpha''=\beta', & \beta''=h''\beta', & \gamma''=\delta', & \delta''=h''\delta'-1 \\
\alpha'''=\beta'', & \beta'''=h'''\beta''-\beta', & \gamma'''=\delta'', & \delta'''=h'''\delta''-\delta' \\
\alpha''''=\beta''', & \beta''''=h''''\beta'''-\beta'', & \gamma''''=\delta''', & \delta''''=h''''\delta'''-\delta''
\end{array}$$
u. s. w.

Dass alle diese Transformationen eigentliche sind, kann ohne Mühe sowohl aus der Bildung derselben als auch aus Artikel 159 abgeleitet werden.

Dieser höchst einfache und zur Rechnung bequeme Algorithmus ist dem im Artikel 27 dargelegten Algorithmus analog und lässt sich auch auf

diesen zurückführen*). Übrigens ist diese Auflösung nicht auf Formen mit negativer Determinante beschränkt, sondern sie erstreckt sich auf alle Fälle, wofern nur keine der Zahlen a', a'', a''', ... gleich Null ist.

178.

Aufgabe. Wenn zwei eigentlich äquivalente Formen F, f mit derselben negativen Determinante gegeben sind, so soll man irgend eine eigentliche Transformation der einen Form in die andere finden.

Auflösung. Wir nehmen an, dass die Form F sei (A, B, A') und dass man nach der Methode des Artikels 171 die Reihe der Formen (A', B', A''), (A'', B'', A'''), ..., $(A^{(m)}, B^{(m)}, A^{(m+1)})$, welche letztere reduciert sei, gefunden habe; ebenso dass die Form f sei (a, b, a') und dass man nach derselben Methode die Reihe der Formen (a', b', a''), (a'', b'', a'''), ..., $(a^{(n)}, b^{(n)}, a^{(n+1)})$, welche letztere reduciert sei, gefunden habe. Dann können zwei Fälle stattfinden.

I. Die Formen $(A^{(m)}, B^{(m)}, A^{(m+1)})$, $(a^{(n)}, b^{(n)}, a^{(n+1)})$ sind entweder identisch oder entgegengesetzt und zugleich ambig. Dann werden die Formen $(A^{(m-1)}, B^{(m-1)}, A^{(m)})$ und $(a^{(n)}, -b^{(n-1)}, a^{(n-1)})$ benachbart sein (wenn $A^{(m-1)}$ das vorletzte Glied der Reihe $A, A', A'', \ldots, A^{(m)}$ bezeichnet und $B^{(m-1)}$, $a^{(n-1)}$, $b^{(n-1)}$ ähnliche Bedeutung haben). Denn es ist $A^{(m)} = a^{(n)}$, $B^{(m-1)} \equiv -B^{(m)}$ (mod. $A^{(m)}$), $b^{(n-1)} \equiv -b^{(n)}$ (mod. $a^{(n)}$ oder $A^{(m)}$), somit $B^{(m-1)} - b^{(n-1)} \equiv b^{(n)} - B^{(m)}$ und daher $\equiv 0$, wenn die Formen $(A^{(m)}, B^{(m)}, A^{(m+1)})$, $(a^{(n)}, b^{(n)}, a^{(n+1)})$ identisch sind, und $\equiv 2b^{(n)}$ und somit $\equiv 0$, wenn sie entgegengesetzt und ambig sind. Daher ist in der Reihe der Formen

$$(A, B, A'), (A', B', A''), \ldots\ldots, (A^{(m-1)}, B^{(m-1)}, A^{(m)}).$$
$$(a^{(n)}, -b^{(n-1)}, a^{(n-1)}), (a^{(n-1)}, -b^{(n-2)}, a^{(n-2)}), \ldots, (a', -b, a), (a, b, a')$$

jede Form der vorhergehenden benachbart, und somit kann nach vorigem Artikel eine eigentliche Transformation der ersten Form F in die letzte f gefunden werden.

---

*) Es wird nämlich in den Zeichen des Artikel 27:

$$\beta^{(n)} = \pm[-h'', h''', -h'''', \ldots, \pm h^{(n)}],$$

wo die doppelt gesetzten Zeichen $--$, $-+$, $+-$, $++$ sein müssen, je nachdem n von der Form $4k+0$, 1, 2, 3 ist; und

$$\delta^{(n)} = \pm[h', -h'', h''', \ldots, \pm h^{(n)}],$$

wo die doppelten Zeichen in der Zusammenstellung $+-$, $++$, $--$, $-+$ genommen werden müssen, je nachdem n von der Form $4k+0$, 1, 2, 3 ist. Doch gestattet uns die Kürze nicht, dies, das übrigens jeder leicht selbst bestätigen kann, weitläufiger zu entwickeln.

II. Die Formen $(A^{(m)}, B^{(m)}, A^{(m+1)})$, $(a^{(n)}, b^{(n)}, a^{(n+1)})$ sind nicht identisch, sondern entgegengesetzt und zugleich $A^{(m)} = A^{(m+1)} = a^{(n)} = a^{(n+1)}$. Dann wird die Reihe der Formen

$$(A, B, A'), (A', B', A''), \ldots\ldots, (A^{(m)}, B^{(m)}, A^{(m+1)}),$$
$$(a^{(n)}, -b^{(n-1)}, a^{(n-1)}), (a^{(n-1)}, -b^{(n-2)}, a^{(n-2)}), \ldots\ldots, (a', -b, a), (a, b, a')$$

dieselbe Eigenschaft besitzen. Denn es ist $A^{(m+1)} = a^{(n)}$, und $B^{(m)} - b^{(n-1)} = -(b^{(n)} + b^{(n-1)})$ ist durch $a^{(n)}$ teilbar. Somit lässt sich nach dem vorigen Artikel eine eigentliche Transformation der ersten Form F in die letzte f finden.

Beispiel. So hat man für die Formen (23, 38, 63), (15, 20, 27) die Reihe:

(23, 38, 63), (63, 25, 10), (10, 5, 3), (3, 1, 2), (2, —7, 27), (27, —20, 15), (15, 20, 27).

Daher ist:

$$h' = 1,\quad h'' = 3,\quad h''' = 2,\quad h'''' = -3,\quad h''''' = -1,\quad h'''''' = 0.$$

Hieraus leitet man als Transformation der Form $23x^2 + 76xy + 63y^2$ in $15t^2 + 40tu + 27u^2$ die folgende ab: $x = -13t - 18u$, $y = 8t + 11u$.

Aus dieser Auflösung folgt ohne Mühe die Auflösung der **Aufgabe:** Wenn die Formen F, f uneigentlich äquivalent sind, so soll man eine uneigentliche Transformation der Form F in f finden. Denn ist $f = at^2 + 2btu + a'u^2$, so ist die entgegengesetzte Form $ap^2 - 2bpq + a'q^2$ der Form F eigentlich äquivalent. Man suche eine eigentliche Transformation der Form F in jene, nämlich $x = \alpha p + \beta q$, $y = \gamma p + \delta q$, so wird offenbar F in f übergehen, wenn man setzt: $x = \alpha t - \beta u$, $y = \gamma t - \delta u$, und diese Transformation wird uneigentlich sein.

Wenn also die Formen F, f sowohl eigentlich als uneigentlich äquivalent sind, so lässt sich immer sowohl eine eigentliche als auch eine uneigentliche Transformation finden.

179.

Aufgabe. Wenn die Formen F, f äquivalent sind, so soll man sämtliche Transformationen von F in f finden.

Auflösung. Wenn die Formen F, f nur auf eine einzige Art, d. h. nur eigentlich oder nur uneigentlich, äquivalent sind, so suche man dem vorigen Artikel gemäss eine Transformation der Form F in f; dann ist klar, dass es andere Transformationen als solche, die dieser gleichartig sind, nicht geben kann. Wenn aber die Formen F, f sowohl eigentlich als uneigentlich äquivalent sind, so suche man zwei Transformationen, eine eigentliche und eine uneigentliche. Ist nun die Form $F = (A, B, C)$, ferner $B^2 - AC = -D$ und der grösste gemeinschaftliche Teiler der Zahlen A, $2B$, C gleich m, so folgt aus Artikel 162, dass im ersteren Falle sämtliche Transformationen

der Form F in f aus einer Transformation, im letzteren Falle alle eigentlichen Transformationen aus der eigentlichen und alle uneigentlichen Transformationen aus der uneigentlichen hergeleitet werden können, wofern man nur sämtliche Lösungen der Gleichung $t^2 + Du^2 = m^2$ hat. Sind diese also gefunden, so ist die Aufgabe gelöst.

Man hat aber $D = AC - B^2$, $4D = 4AC - 4B^2$, somit ist $\frac{4D}{m^2} = 4\frac{AC}{m^2} - \left(\frac{2B}{m}\right)^2$ eine ganze Zahl. Wenn nun

1. $\frac{4D}{m^2} > 4$ ist, so ist $D > m^2$, daher muss in $t^2 + Du^2 = m^2$ notwendig $u = 0$ sein, und somit kann t keine andern Werte als $+m$ oder $-m$ haben. Wenn daher F, f nur auf eine einzige Weise äquivalent sind und irgend eine Transformation

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

ist, so kann es ausser dieser, welche aus $t = m$ entsteht (Artikel 162), und der folgenden

$$x = -\alpha x' - \beta y', \quad y = -\gamma x' - \delta y'$$

keine Transformationen weiter geben. Wenn aber F, f sowohl eigentlich als auch uneigentlich äquivalent sind, und man irgend eine eigentliche Transformation

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

und eine uneigentliche

$$x = \alpha' x' + \beta' y', \quad y = \gamma' x' + \delta' y'$$

hat, so wird es ausser jener (aus $t = m$ entstehenden) und der folgenden (aus $t = -m$ entstehenden)

$$x = -\alpha x' - \beta y', \quad y = -\gamma x' - \delta y'$$

keine eigentliche und in analoger Weise keine uneigentliche Transformation weiter geben ausser

$$x = \alpha' x' + \beta' y', \; y = \gamma' x' + \delta' y'; \text{ und } x = -\alpha' x' - \beta' y', \; y = -\gamma' x' - \delta' y'.$$

2. Ist $\frac{4D}{m^2} = 4$ oder $D = m^2$, so lässt die Gleichung $t^2 + Du^2 = m^2$ vier Lösungen zu, nämlich: $t, u = m, 0; -m, 0; 0, 1; 0, -1$. Wenn demnach F, f nur auf eine einzige Weise äquivalent sind, und irgend eine Transformation lautet:

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y',$$

so giebt es im Ganzen vier Transformationen:

$$x = \pm \alpha x' \pm \beta y', \quad y = \pm \gamma x' \pm \delta y'$$

$$x = \mp \frac{\alpha B + \gamma C}{m} x' \mp \frac{\beta B + \delta C}{m} y', \quad y = \pm \frac{\alpha A + \gamma B}{m} x' \pm \frac{\beta A + \delta B}{m} y'.$$

Wenn dagegen F, f auf zwei Arten äquivalent sind oder es ausser jener gegebenen Transformation noch eine andere ihr ungleichartige giebt, so wird diese ebenfalls vier jenen ungleichartige Transformationen hervorbringen, so dass man acht Tansformationen hat. — Übrigens kann man leicht beweisen, dass in diesem Falle F, f stets wirklich auf zwei Arten äquivalent sind. Denn da $D = m^2 = AC - B^2$ ist, so geht m auch in B auf. Die Determinante der Form $\left(\frac{A}{m}, \frac{B}{m}, \frac{C}{m}\right)$ ist gleich -1, daher ist die Form entweder der Form $(1, 0, 1)$ oder der Form $(-1, 0, -1)$ äquivalent. Man sieht aber leicht, dass durch dieselbe Transformation, durch welche die Form $\left(\frac{A}{m}, \frac{B}{m}, \frac{C}{m}\right)$ in $(\pm 1, 0, \pm 1)$ übergeht, auch (A, B, C) in $(\pm m, 0, \pm m)$, welche ambig ist, übergeht. Daher ist die Form (A, B, C), da sie einer ambigen Form äquivalent ist, jeder ihr überhaupt äquivalenten Form sowohl eigentlich als auch uneigentlich äquivalent.

3. Ist $\frac{4D}{m^2} = 3$ oder $4D = 3m^2$, so ist m gerade, und sämtliche Lösungen der Gleichung $t^2 + Du^2 = m^2$ sind die folgenden sechs:

$$t,\ u = m,\ 0;\quad -m,\ 0;\quad \tfrac{1}{2}m,\ 1;\quad -\tfrac{1}{2}m,\ -1;\quad \tfrac{1}{2}m,\ -1;\quad -\tfrac{1}{2}m,\ 1.$$

Hat man daher zwei ungleichartige Transformationen der Form F in f:

$$x = \alpha x' + \beta y',\quad y = \gamma x' + \delta y'$$
$$x = \alpha' x' + \beta' y',\quad y = \gamma' x' + \delta' y',$$

so hat man zwölf Transformationen, nämlich sechs der ersteren gleichartige:

$$x = \pm \alpha x' \pm \beta y';\quad y = \pm \gamma x' \pm \delta x',$$

$$\begin{cases} x = \pm\left(\tfrac{1}{2}\alpha - \dfrac{\alpha B + \gamma C}{m}\right)x' \pm \left(\tfrac{1}{2}\beta - \dfrac{\beta B + \delta C}{m}\right)y', \\ y = \pm\left(\tfrac{1}{2}\gamma + \dfrac{\alpha A + \gamma B}{m}\right)x' \pm \left(\tfrac{1}{2}\delta + \dfrac{\beta A + \delta B}{m}\right)y'; \end{cases}$$

$$\begin{cases} x = \pm\left(\tfrac{1}{2}\alpha + \dfrac{\alpha B + \gamma C}{m}\right)x' \pm \left(\tfrac{1}{2}\beta + \dfrac{\beta B + \delta C}{m}\right)y', \\ y = \pm\left(\tfrac{1}{2}\gamma - \dfrac{\alpha A + \gamma B}{m}\right)x' \pm \left(\tfrac{1}{2}\delta - \dfrac{\beta A + \delta B}{m}\right)y'; \end{cases}$$

und sechs der letzteren gleichartige, welche aus den vorstehenden erhalten werden, wenn man für $\alpha, \beta, \gamma, \delta$ respective $\alpha', \beta', \gamma', \delta'$ setzt.

Dass aber in diesem Falle stets F, f auf beide Arten äquivalent sind, wird folgendermassen bewiesen: Die Determinante der Form $\left(\frac{2A}{m}, \frac{2B}{m}, \frac{2C}{m}\right)$ ist gleich $-\frac{4D}{m^2} = -3$, und demnach ist diese Form (Artikel 176) entweder der Form $(\pm 1, 0, \pm 3)$ oder der folgenden Form $(\pm 2, \pm 1, \pm 2)$ äquivalent. Hieraus ist leicht ersichtlich, dass die Form (A, B, C) entweder der Form

$(\pm \frac{1}{2}m,\ 0,\ \pm \frac{3}{2}m)$ oder der Form $(\pm m,\ \frac{1}{2}m,\ \pm m)$*), welche beide ambig sind, äquivalent und somit jeder ihr überhaupt äquivalenten Form auf beide Arten äquivalent ist.

4. Nimmt man an, dass $\frac{4D^2}{m^2} = 2$ sei, so wird $\left(\frac{2B}{m}\right)^2 = 4\frac{AC}{m^2} - 2$ und daher $\equiv 2 \pmod{4}$. Da aber kein Quadrat $\equiv 2 \pmod{4}$ sein kann, so kann dieser Fall nicht stattfinden.

5. Nimmt man an, dass $\frac{4D}{m^2} = 1$ sei, so wird $\left(\frac{2B}{m}\right)^2 = 4\frac{AC}{m^2} - 1 \equiv -1 \pmod{4}$. Da dies aber unmöglich ist, so kann auch dieser Fall nicht stattfinden.

Da ferner D weder gleich Null noch negativ ist, so kann es andere Fälle als die aufgezählten nicht geben.

180.

Aufgabe. Man soll alle Darstellungen einer gegebenen Zahl M durch die Form $ax^2 + 2bxy + cy^2$ oder F mit der negativen Determinante $-D$ finden, in denen x, y unter einander prime Werte erhalten.

Auflösung. Aus Artikel 154 geht hervor, dass M auf die gewünschte Art nur dargestellt werden kann, wenn $-D$ quadratischer Rest von M ist. Man suche daher zunächst alle verschiedenen (d. h. incongruenten) Werte des Ausdrucks $\sqrt{-D} \pmod{M}$, welche $N, -N, N', -N', N'', -N''\ldots$ seien. Damit die Rechnung möglichst einfach werde, können alle $N, N'\ldots$ so bestimmt werden, dass sie nicht grösser als $\frac{1}{2}M$ sind. Da nun jede Darstellung zu irgend einem dieser Werte gehören muss, mögen die einzelnen Werte gesondert betrachtet werden.

Wenn die Formen F und $\left(M,\ N,\ \frac{D+N^2}{M}\right)$ nicht eigentlich äquivalent sind, so kann es keine Darstellung von M geben, welche zum Werte N gehört (Artikel 168). Sind sie dagegen eigentlich äquivalent, so suche man eine eigentliche Transformation der Form F in

$$Mx'^2 + 2Nx'y' + \frac{D+N^2}{M}y'^2,$$

welche

$$x = \alpha x' + \beta y',\ y = \gamma x' + \delta y'$$

sein möge, so ist $x = \alpha$, $y = \gamma$ die zu N gehörige Darstellung der Zahl M durch F. Es sei der grösste gemeinschaftliche Teiler der Zahlen A, $2B$, C gleich m und man unterscheide drei Fälle (vgl. vorigen Artikel):

*) Man kann zeigen, dass die Form $(A,\ B,\ C)$ notwendig der letzteren äquivalent ist; doch ist dies hier nicht nötig.

1. Ist $\frac{4D}{m^2} > 4$, so kann es andere zu N gehörige Darstellungen nicht geben als die folgenden beiden: $x = \alpha$, $y = \gamma$; $x = -\alpha$, $y = -\gamma$ (Artikel 169, 179).

2. Ist $\frac{4D}{m^2} = 4$, so hat man die vier Darstellungen:

$$x = \pm\alpha,\ y = \pm\gamma;\ x = \mp\frac{\alpha B + \gamma C}{m},\ y = \pm\frac{\alpha A + \gamma B}{m}$$

3. Ist $\frac{4D}{m^2} = 3$, so hat man die sechs Darstellungen:

$$x = \pm\alpha, \qquad y = \pm\gamma$$
$$x = \pm\left(\tfrac{1}{2}\alpha - \frac{\alpha B + \gamma C}{m}\right), \quad y = \pm\left(\tfrac{1}{2}\gamma + \frac{\alpha A + \gamma B}{m}\right)$$
$$x = \pm\left(\tfrac{1}{2}\alpha + \frac{\alpha B + \gamma C}{m}\right), \quad y = \pm\left(\tfrac{1}{2}\gamma - \frac{\alpha A + \gamma B}{m}\right).$$

In derselben Weise sind die zu den Werten $-N$, N', $-N'$, ... gehörigen Darstellungen zu suchen.

181.

Die Ermittelung der Darstellungen einer Zahl M durch die Form F, in welchen x, y einander nicht prime Werte haben, lässt sich auf den bereits betrachteten Fall leicht zurückführen. Man möge eine solche Darstellung erhalten, wenn man setzt $x = \mu e$, $y = \mu f$, wo μ der grösste gemeinschaftliche Teiler von μe und μf ist, d. h. e und f zu einander prim sind. Die Substitution $x = e$, $y = f$ wird aber die Darstellung der Zahl $\frac{M}{\mu^2}$ durch die Form F sein, in welcher x, y zu einander prime Werte haben. Wenn daher M durch keine Quadratzahl (ausser 1) teilbar ist, z. B. wenn es eine Primzahl ist, so giebt es keine solche Darstellungen von M. Wenn aber M quadratische Teiler enthält, so mögen diese μ^2, ν^2, π^2, ... sein. Man suche zunächst alle Darstellungen der Zahl $\frac{M}{\mu^2}$ durch die Form (A, B, C), in denen x, y zu einander prime Werte haben; diese Werte werden, mit μ multipliciert, alle Darstellungen von M ergeben, in welchen der grösste gemeinschaftliche Teiler von x, y gleich μ ist. In ähnlicher Weise werden alle Darstellungen von $\frac{M}{\nu^2}$, in denen die Werte von x, y prim zu einander sind, alle Darstellungen von M ergeben, in welchen der grösste gemeinschaftliche Teiler von x, y gleich ν ist, u. s. w.

Es ist daher klar, dass durch die vorstehenden Regeln sämtliche Darstellungen einer gegebenen Zahl durch eine gegebene Form mit negativer Determinante gefunden werden können.

Specielle Anwendungen auf die Zerlegung der Zahlen in zwei Quadrate, in ein einfaches und ein doppeltes und in ein einfaches und ein dreifaches Quadrat.

182.

Wir gehen zu einigen besonderen Fällen über einmal wegen ihrer hervorragenden Eleganz, sodann weil sich Euler mit ihnen eingehend beschäftigt hat, wodurch sie gewissermassen klassisches Ansehen erhalten haben.

I. Durch die Form x^2+y^2 kann so, dass x zu y prim ist, keine Zahl dargestellt (oder in zwei zu einander prime Quadrate zerlegt) werden, von welcher nicht -1 quadratischer Rest ist; dagegen ist dies auch bei allen solchen, positiv genommenen, Zahlen wirklich möglich. Es sei M eine solche Zahl und es seien N, $-N$, N', $-N'$, N'', $-N''$, ... die sämtlichen Werte des Ausdrucks $\sqrt{-1}$ (mod. M). Dann ist nach Artikel 176 die Form $\left(M, N, \frac{N^2+1}{M}\right)$ der Form $(1, 0, 1)$ eigentlich äquivalent. Ist $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ irgend eine eigentliche Transformation dieser Form in jene, so sind die zu N gehörigen Darstellungen der Zahl M durch die Form x^2+y^2 die folgenden vier*): $x = \pm\alpha$, $y = \pm\gamma$; $x = \mp\gamma$, $y = \pm\alpha$.

Da die Form $(1, 0, 1)$ ambig ist, so wird offenbar auch die Form $\left(M, -N, \frac{N^2+1}{M}\right)$ derselben eigentlich äquivalent sein und jene eigentlich in diese transformiert werden, wenn man setzt: $x = \alpha x' - \beta y'$, $y = -\gamma x' + \delta y'$. Hieraus ergeben sich vier zu $-N$ gehörende Darstellungen von M, nämlich $x = \pm\alpha$, $y = \mp\gamma$; $x = \pm\gamma$, $y = \pm\alpha$. Es ist somit klar, dass es acht Darstellungen von M giebt, von denen die eine Hälfte zu N, die andere Hälfte zu $-N$ gehört; aber alle diese stellen nur eine einzige Zerlegung der Zahl M in zwei Quadrate dar: $M = \alpha^2 + \gamma^2$, wofern man nämlich nur die Quadrate selbst, nicht aber auch ihre Reihenfolge oder die Vorzeichen ihrer Wurzeln in Betracht zieht.

Wenn es daher keine andern Werte des Ausdrucks $\sqrt{-1}$ (mod. M) ausser N und $-N$ giebt, was z. B. der Fall ist, wenn M eine Primzahl ist, so lässt sich M nur auf eine einzige Weise in zwei zu einander prime Quadrate zerlegen. Da nun -1 quadratischer Rest einer jeden Primzahl von der Form $4n+1$ ist (Artikel 108) und eine Primzahl in zwei zu einander nicht prime Quadrate offenbar nicht zerlegt werden kann, so haben wir den **Satz**:

Jede Primzahl von der Form $4n+1$ kann in zwei Quadrate zerlegt werden und zwar nur auf eine einzige Weise.

---

*) Offenbar nämlich ist dieser Fall unter Artikel 180, 2 enthalten.

So ist: $1 = 0 + 1$, $5 = 1 + 4$, $13 = 4 + 9$, $17 = 1 + 16$, $29 = 4 + 25$, $37 = 1 + 36$, $41 = 16 + 25$, $53 = 4 + 49$, $61 = 25 + 36$, $73 = 9 + 64$, $89 = 25 + 64$, $97 = 16 + 81$, ...

Dieser höchst elegante Satz war schon Fermat bekannt, doch wurde er zuerst von Euler bewiesen: *Comm. nov. Petr. T. V für die Jahre 1754, 1755 S. 3 u. ff.* Im vierten Bande S. 3 u. ff. findet sich eine denselben Gegenstand betreffende Abhandlung, doch hatte er damals die Sache noch nicht vollständig erledigt, vgl. besonders Artikel 27.

Wenn daher irgend eine Zahl von der Form $4n + 1$ entweder auf mehrere Arten oder gar nicht in zwei Quadrate zerlegt werden kann, so ist sie sicher keine Primzahl.

Umgekehrt aber wird es, wenn der Ausdruck $\sqrt{-1}$ (mod. M) ausser N und $-N$ noch andere Werte hat, auch noch andere zu diesen Werten gehörende Darstellungen von M geben. In diesem Falle wird also M auf mehrere Arten in zwei Quadrate zerlegt werden können, z. B. $65 = 1 + 64 = 16 + 49$, $221 = 25 + 196 = 100 + 121$.

Die übrigen Darstellungen, in welchen x, y zu einander nicht prime Werte erhalten, können nach unserer allgemeinen Methode leicht gefunden werden. Wir bemerken nur, dass, wenn irgend eine Zahl, welche Factoren von der Form $4n + 3$ enthält, von diesen durch keine Division durch ein Quadrat befreit werden kann (was der Fall ist, wenn einer oder mehrere dieser Factoren in ungerader Potenz vorkommen), diese auf keine Weise in zwei Quadrate zerlegt werden kann*).

II. Durch die Form $x^2 + 2y^2$ lässt sich keine Zahl, von welcher -2 Nichtrest ist, so darstellen, dass x zu y prim ist, während dies bei allen andern möglich ist. Ist -2 Rest der Zahl M und N irgend ein Wert des Ausdrucks $\sqrt{-2}$ (mod. M), so werden nach Artikel 176 die Formen $(1, 0, 2)$ und $\left(M, N, \frac{N^2+2}{M}\right)$ eigentlich äquivalent sein. Geht jene eigentlich in diese über, wenn man setzt $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, so wird $x = \alpha$, $y = \gamma$ die zu N gehörige Darstellung der Zahl M sein. Ausser dieser und der folgenden $x = -\alpha$, $y = -\gamma$ gehören keine andern zu N (Artikel 180).

*) Ist die Zahl $M = 2^\mu S a^\alpha b^\beta c^\gamma \ldots$, so dass $a, b, c, \ldots$ ungleiche Primzahlen von der Form $4n + 1$ sind und S das Product aus allen Primfactoren von M von der Form $4n + 3$ ist (auf welche Form jede positive Zahl reduciert werden kann, wenn man, falls M ungerade ist, $\mu = 0$ und, falls M keine Factoren von der Form $4n + 3$ enthält, $S = 1$ setzt), so kann M auf keine Weise in zwei Quadrate zerlegt werden, wenn nicht S ein Quadrat ist. Ist aber S ein Quadrat, so giebt es $\frac{1}{2}(\alpha + 1)(\beta + 1)(\gamma + 1) \ldots$ Zerlegungen von M, falls eine der Zahlen $\alpha, \beta, \gamma, \ldots$ ungerade ist, oder $\frac{1}{2}(\alpha + 1)(\beta + 1)(\gamma + 1) \cdots + \frac{1}{2}$, falls $\alpha, \beta, \gamma, \ldots$ sämtlich gerade sind (wofern man nur die Quadrate selbst in Betracht zieht). Wer in der Combinationsrechnung einigermassen geübt ist, wird den Beweis dieses Satzes (bei dem wir uns, ebenso wie bei anderen Einzelheiten, nicht aufhalten können) aus unserer allgemeinen Theorie ohne Schwierigkeit ableiten können.

Analog wie oben erkennt man, dass die Darstellungen $x = \pm\alpha$, $y = \mp\gamma$ zum Werte $-N$ gehören. Alle diese vier Darstellungen aber ergeben nur eine einzige Zerlegung von M in ein Quadrat und das Doppelte eines Quadrats, und wenn es ausser N und $-N$ keine andern Werte des Ausdrucks $\sqrt{-2}\,(\text{mod.}\,M)$ weiter giebt, so giebt es auch keine andern Darstellungen von M. Hieraus leitet man mit Hülfe des Satzes in Artikel 116 leicht den **Satz** her:

Jede Primzahl von der Form $8n+1$ oder $8n+3$ lässt sich in ein Quadrat und ein doppeltes Quadrat zerlegen und zwar nur auf eine einzige Weise.

So ist z. B. $1 = 1 + 0$, $3 = 1 + 2$, $11 = 9 + 2$, $17 = 9 + 8$, $19 = 1 + 18$, $41 = 9 + 32$, $43 = 25 + 18$, $59 = 9 + 50$, $67 = 49 + 18$, $73 = 1 + 72$, $83 = 81 + 2$, $89 = 81 + 8$, $97 = 25 + 72$, u. s. w.

Auch diesen Satz, wie mehrere ähnliche, kannte Fermat, doch gab Lagrange zuerst einen Beweis. *Suite des recherches d'Arithmétique, Nouv. Mém. de l'Ac. de Berlin 1775, p. 323 u. ff.* Manches auf diesen Gegenstand Bezügliche hatte schon Euler erledigt, *Specimen de usu observationum in mathesi pura, Comm. nov. Petr. T. VI, p. 185 u. ff.*, aber der vollständige Beweis des Satzes spottete stets seinen Bemühungen. Vergleiche auch die Abhandlung in T. VIII (zu den Jahren 1760, 1761): *Supplementum quorundam theorematum arithmeticorum,* am Schluss.

III. Auf ähnlichem Wege beweist man, dass jede Zahl, von welcher -3 quadratischer Rest ist, sich darstellen lässt entweder durch die Form $x^2 + 3y^2$ oder durch die folgende: $2x^2 + 2xy + 2y^2$ und zwar so, dass der Wert von x prim zum Werte von y ist. Da nun -3 Rest aller Primzahlen von der Form $3n + 1$ ist (Artikel 119) und durch die Form $2x^2 + 2xy + 2y^2$ augenscheinlich nur gerade Zahlen dargestellt werden können, so hat man wie oben den **Satz:**

Jede Primzahl von der Form $3n + 1$ lässt sich in ein Quadrat und ein dreifaches Quadrat zerlegen und zwar nur auf eine einzige Weise.

So ist z. B. $1 = 1 + 0$, $7 = 4 + 3$, $13 = 1 + 12$, $19 = 16 + 3$, $31 = 4 + 27$, $37 = 25 + 12$, $43 = 16 + 27$, $61 = 49 + 12$, $67 = 64 + 3$, $73 = 25 + 48$, u. s. w.

Den Beweis dieses Satzes hat zuerst Euler angegeben in der eben erwähnten Abhandlung, *Comm. nov. Petrop. T. VIII, p. 105 u. ff.*

In ähnlicher Weise könnten wir weiter gehen und z. B. zeigen, dass jede Primzahl von der Form $20n + 1$ oder $20n + 3$ oder $20n + 7$ oder $20n + 9$ (von denen nämlich -5 Rest ist) durch eine der beiden Formen $x^2 + 5y^2$, $2x^2 + 2xy + 3y^2$ dargestellt werden kann und zwar die Primzahlen von der Form $20n + 1$ und $20n + 9$ durch die erstere, die Primzahlen von der Form $20n + 3$, $20n + 7$ durch die letztere Form; ferner das Doppelte der Primzahlen von der Form $20n + 1$, $20n + 9$ durch die

Form $2x^2 + 2xy + 3y^2$, das Doppelte der Primzahlen von der Form $20n + 3$, $20n + 7$ aber durch die Form $x^2 + 5y^2$. Indessen wird jeder diesen Satz und unzählig viele andere specielle Sätze aus dem Vorhergehenden und dem, was weiter unten auseinandergesetzt werden wird, leicht selbst ableiten können. — Wir gehen daher zu den Formen mit positiver Determinante über, und da deren Natur eine ganz andere ist, je nachdem die Determinante eine Quadratzahl oder eine nichtquadratische Zahl ist, so schliessen wir hier zunächst die Formen mit quadratischer Determinante aus und werden dieselben später gesondert betrachten.

Von den Formen mit positiver nichtquadratischer Determinante.

183.

Aufgabe. Wenn eine beliebige Form (a, b, a') gegeben ist, deren positive nichtquadratische Determinante gleich D ist, so soll man eine dieser eigentlich äquivalente Form (A, B, C) finden, in welcher B positiv und kleiner als $\sqrt{D}$ ist, A dagegen, falls es positiv ist, oder $-A$, falls A negativ ist, zwischen $\sqrt{D} + B$ und $\sqrt{D} - B$ liegt.

Auflösung. Wir nehmen an, dass in der gegebenen Form noch nicht beide Bedingungen erfüllt seien, denn sonst brauchten wir eine andere Form nicht zu suchen. Ferner bemerken wir, dass in einer Form mit nichtquadratischer Determinante das erste oder letzte Glied nicht gleich Null sein kann (Artikel 171, Anm.). Es sei $b' \equiv -b \pmod{a'}$ und zwischen den Grenzen $\sqrt{D}$ und $\sqrt{D} \mp a'$ gelegen (wo das obere Zeichen genommen wird, wenn a' positiv, das untere, wenn es negativ ist). Dass dies möglich ist, beweist man leicht in ähnlicher Weise, wie in Artikel 3. Man setze sodann $\frac{b'^2 - D}{a'} = a''$, welches eine ganze Zahl ist, da $b'^2 - D \equiv b^2 - D \equiv aa' \equiv 0 \pmod{a'}$ ist. Ist nun $a'' < a'$, so sei wiederum $b'' \equiv -b' \pmod{a''}$ und zwischen $\sqrt{D}$ und $\sqrt{D} \mp a''$ (je nachdem a'' positiv oder negativ ist) gelegen und ferner $\frac{b''^2 - D}{a''} = a'''$. Ist hier wiederum $a''' < a''$, so sei $b''' = -b'' \pmod{a'''}$ und zwischen $\sqrt{D}$ und $\sqrt{D} \mp a'''$ gelegen und $\frac{b'''^2 - D}{a'''} = a''''$. Diese Operation setze man fort, bis man in der Reihe a', a'', a''', a'''', ... zu einem Gliede $a^{(m+1)}$ gelangt, welches nicht kleiner ist als das vorhergehende $a^{(m)}$, was endlich eintreten muss, weil man sonst eine unendliche Reihe beständig abnehmender ganzer Zahlen haben würde. Setzt man dann $a^{(m)} = A$, $b^{(m)} = B$, $a^{(m+1)} = C$, so wird die Form (A, B, C) allen Bedingungen genügen.

Beweis. I. Da in der Reihe der Formen (a, b, a'), (a', b', a''), (a'', b'', a'''), ... eine jede der vorhergehenden benachbart ist, wird die letzte (A, B, C) der ersten (a, b, a') eigentlich äquivalent sein.

II. Da B zwischen $\sqrt{D}$ und $\sqrt{D} \mp A$ liegt (wo stets das obere Zeichen, wenn A positiv, das untere, wenn A negativ ist, zu nehmen ist), so werden offenbar, wenn man $\sqrt{D} - B = p$, $B - (\sqrt{D} \mp A) = q$ setzt, diese Grössen p, q positiv sein. Nun bestätigt man leicht, dass $q^2 + 2pq + 2p\sqrt{D} = D + A^2 - B^2$ ist; somit wird $D + A^2 - B^2$ eine positive Zahl sein, die wir gleich r setzen. Hiernach wird, da $D = B^2 - AC$ ist, $r = A^2 - AC$, und demnach ist $A^2 - AC$ eine positive Zahl. Weil aber nach Voraussetzung A nicht grösser ist als C, so kann jenes offenbar nicht anders stattfinden, als wenn AC negativ ist und daher die Vorzeichen von A und C entgegengesetzt sind. Hieraus folgt $B^2 = D + AC < D$ und somit $B < \sqrt{D}$.

III. Da ferner $-AC = D - B^2$ ist, so wird $AC < D$ und daher (weil A nicht grösser als C) $A < \sqrt{D}$. Somit ist $\sqrt{D} \mp A$ positiv, also auch B, welches zwischen den Grenzen $\sqrt{D}$ und $\sqrt{D} \mp A$ gelegen ist.

IV. Somit ist umsomehr $\sqrt{D} + B \mp A$ positiv, und da $\sqrt{D} - B \mp A = -q$ negativ ist, so ist $\pm A$ zwischen $\sqrt{D} + B$ und $\sqrt{D} - B$ gelegen.

Beispiel. Ist die Form (67, 97, 140), deren Determinante gleich 29 ist, gegeben, so findet man hier die Reihe der Formen: (67, 97, 140), (140, −97, 67), (67, −37, 20), (20, −3, −1), (−1, 5, 4). Die letzte ist die gesuchte.

Derartige Formen (A, B, C) mit der positiven nichtquadratischen Determinante D, in welchen A, positiv genommen, zwischen $\sqrt{D} + B$ und $\sqrt{D} - B$ liegt, B aber positiv und kleiner als $\sqrt{D}$ ist, werden wir **reducierte Formen** nennen. Die reducierten Formen mit positiver nichtquadratischer Determinante unterscheiden sich daher etwas von den reducierten Formen mit negativer Determinante; wegen der grossen Analogie zwischen diesen und jenen aber wollten wir keine verschiedenen Benennungen einführen.

184.

Wenn die Äquivalenz zweier reducierten Formen mit positiver Determinante ebenso leicht beurteilt werden könnte, wie bei den Formen mit negativer Determinante (Artikel 172), so würde man die Äquivalenz zweier beliebigen Formen mit derselben positiven Determinante ohne Mühe erkennen können. Aber hier verhält sich die Sache bei weitem anders, und es ist möglich, dass sehr viele reducierte Formen unter einander äquivalent sind. Bevor wir daher an diese Aufgabe herantreten, müssen wir erst tiefer in die Natur der reducierten Formen (mit positiver nichtquadratischer Determinante, was man hier immer hinzudenken muss) eindringen.

1. Ist (a, b, c) eine reducierte Form, so haben a und c entgegengesetzte Vorzeichen. Denn setzt man die Determinante der Form gleich D, so ist $ac = b^2 - D$ und daher negativ, weil $b < \sqrt{D}$ ist.

2. Die Zahl c ist ebenso wie a, positiv genommen, zwischen $\sqrt{D} + b$ und $\sqrt{D} - b$ gelegen. Denn es ist $-c = \frac{D - b^2}{a}$; daher liegt c, abgesehen vom Vorzeichen, zwischen $\frac{D - b^2}{\sqrt{D} + b}$ und $\frac{D - b^2}{\sqrt{D} - b}$, d. h. zwischen $\sqrt{D} - b$ und $\sqrt{D} + b$.

3. Hieraus geht hervor, dass auch (c, b, a) eine reducierte Form ist.

4. Sowohl a wie c ist kleiner als $2\sqrt{D}$. Jedes der beiden nämlich ist kleiner als $\sqrt{D} + b$ und daher umsomehr kleiner als $2\sqrt{D}$.

5. Die Zahl b liegt zwischen $\sqrt{D}$ und $\sqrt{D} \mp a$ (wo das obere Zeichen bei positivem a, das untere bei negativem a zu nehmen ist). Denn da $\pm a$ zwischen $\sqrt{D} + b$ und $\sqrt{D} - b$ liegt, so ist $\pm a - (\sqrt{D} - b)$ oder $b - (\sqrt{D} \mp a)$ positiv; $b - \sqrt{D}$ aber ist negativ; mithin liegt b zwischen $\sqrt{D}$ und $\sqrt{D} \mp a$. — Ganz auf dieselbe Weise wird bewiesen, dass b zwischen $\sqrt{D}$ und $\sqrt{D} \mp c$ (je nachdem c positiv oder negativ ist) liegt.

6. Jeder reducierten Form (a, b, c) ist nach jeder der beiden Seiten hin eine und nur eine reducierte Form benachbart.

Ist $a' = c$, $b' \equiv -b \pmod{a'}$ und zwischen $\sqrt{D}$ und $\sqrt{D} \mp a'$*) gelegen, ferner $c' = \frac{b'^2 - D}{a'}$, so ist die Form (a', b', c') der Form (a, b, c) nach rechts hin benachbart und zugleich ist klar, dass, wenn es irgend eine reducierte der Form (a, b, c) nach rechts hin benachbarte Form gäbe, dieselbe von (a', b', c') nicht verschieden sein kann. Dass aber diese wirklich reduciert ist, beweisen wir folgendermassen.

A) Setzt man

$$\sqrt{D} + b \mp a' = p, \quad \pm a' - (\sqrt{D} - b) = q, \quad \sqrt{D} - b = r,$$

so sind diese Zahlen p, q, r nach (2) oben und nach der Erklärung der reducierten Form positiv. Setzt man ferner

$$b' - (\sqrt{D} \mp a') = q', \quad \sqrt{D} - b' = r',$$

so sind q', r' positiv, da b' zwischen $\sqrt{D}$ und $\sqrt{D} \mp a'$ liegt. Ist endlich $b + b' = \pm ma'$, so ist m eine ganze Zahl. Nun ist offenbar $p + q' = b + b'$ und daher $b + b'$ oder $\pm ma'$ und somit auch m positiv. Hieraus folgt, dass $m - 1$ sicher nicht negativ ist. Ferner wird:

---

*) Wo Doppelzeichen vorkommen, gilt stets das obere, wenn a' positiv, das untere, wenn a' negativ ist.

$$r + q' \pm ma' = 2b' \pm a' \text{ oder } 2b' = r + q' \pm (m-1)\,a',$$

mithin sind $2b'$ und b' notwendig positiv; und da $b' + r' = \sqrt{D}$, so ist $b' < \sqrt{D}$.

B) Ferner wird:

$$r \pm ma' = \sqrt{D} + b', \text{ oder } r \pm (m-1)\,a' = \sqrt{D} + b' \mp a',$$

mithin ist $\sqrt{D} + b' \mp a'$ positiv. Hieraus und weil $\pm a' - \left(\sqrt{D} - b'\right) = q'$ und somit positiv ist, folgt, dass $\pm a'$ zwischen $\sqrt{D} + b'$ und $\sqrt{D} - b'$ liegt. — Demnach ist (a', b', c') eine reducierte Form.

Auf dieselbe Art beweist man, dass, wenn $'c = a$, $'b \equiv -b \pmod{'c}$ ist und zwischen $\sqrt{D}$ und $\sqrt{D} \pm 'c$ liegt, ferner $'a = \dfrac{'b^2 - D}{'c}$ ist, die Form $('a, 'b, 'c)$ eine reducierte ist. Offenbar aber ist diese Form der Form (a, b, c) nach links hin benachbart und eine andere reducierte Form ausser $('a, 'b, 'c)$ kann diese Eigenschaft nicht besitzen.

Beispiel. Der reducierten Form $(5, 11, -14)$, deren Determinante gleich 191 ist, ist nach rechts hin die reducierte Form $(-14, 3, 13)$, nach links hin aber die folgende $(-22, 9, 5)$ benachbart.

7. Wenn der reducierten Form (a, b, c) die reducierte Form (a', b', c') nach rechts hin benachbart ist, so wird der reducierten Form (c, b, a) die Form (c', b', a') nach links hin benachbart sein; und wenn der reducierten Form (a, b, c) die Form $('a, 'b, 'c)$ nach links hin benachbart ist, so wird die reducierte Form $('c, 'b, 'a)$ der reducierten Form (c, b, a) nach rechts hin benachbart sein. Ferner werden auch die Formen $(-'a, 'b, -'c)$ $(-a, b, -c)$, $(-a', b', -c')$ reducierte sein und zwar ist die zweite der ersten, die dritte der zweiten nach rechts hin oder die erste der zweiten, die zweite der dritten nach links hin benachbart, und ähnlich verhält es sich mit den drei Formen $(-c', b', -a')$, $(-c, b, -a)$, $(-'c, 'b, -'a)$. Dies ist so klar, dass es einer Auseinandersetzung nicht bedarf.

185.

Die Anzahl aller reducierten Formen mit gegebener Determinante D ist stets eine endliche; sie selbst aber können auf zwiefache Weise gefunden werden. Wir wollen unbestimmt alle reducierten Formen mit der Determinante D durch (a, b, c) bezeichnen, so dass sämtliche Werte von a, b, c bestimmt werden müssen.

Erste Methode. Man nehme für a alle Zahlen (sowohl positiv als negativ), welche kleiner als $2\sqrt{D}$ sind und von denen D quadratischer Rest ist, und setze für jedes einzelne a die Zahl b gleich sämtlichen positiven Werten des Ausdrucks $\sqrt{D} \pmod{a}$, welche zwischen $\sqrt{D}$ und $\sqrt{D} \mp a$ liegen, c aber setze man für die einzelnen bestimmten Werte von a, b gleich

$\frac{b^2 - D}{a}$. Wenn sich auf diese Weise irgend welche Formen ergeben, in denen $\pm a$ ausserhalb des Intervalles $\sqrt{D} + b$ und $\sqrt{D} - b$ liegt, so sind dieselben zu verwerfen.

Zweite Methode. Man nehme für b alle positiven Zahlen, welche kleiner als $\sqrt{D}$ sind, zerlege für die einzelnen b den Ausdruck $b^2 - D$ auf alle möglichen Weisen in zwei Factoren, welche absolut genommen zwischen $\sqrt{D} + b$ und $\sqrt{D} - b$ liegen und setze den einen gleich a den andern gleich c. Offenbar giebt jede einzelne Zerlegung in Factoren zwei Formen, weil jeder der beiden Factoren sowohl gleich a wie gleich c gesetzt werden muss.

Beispiel. Ist $D = 79$, so werden die Werte von a die folgenden zweiundzwanzig sein: $\mp 1, 2, 3, 5, 6, 7, 9, 10, 13, 14, 15$. Hieraus findet man neunzehn Formen:

$$(1, 8, -15), (2, 7, -15), (3, 8, -5), (3, 7, -10), (5, 8, -3), (5, 7, -6),$$
$$(6, 7, -5), (6, 5, -9), (7, 4, -9), (7, 3, -10), (9, 5, -6), (9, 4, -7),$$
$$(10, 7, -3), (10, 3, -7), (13, 1, -6), (14, 3, -5), (15, 8, -1), (15, 7, -2),$$
$$(15, 2, -5),$$

und ebenso viele andere, welche aus diesen entstehen, wenn man die Vorzeichen der äusseren Glieder ändert, nämlich $(-1, 8, 15)$, $(-2, 7, 15), \ldots$, so dass es im ganzen achtunddreissig giebt. Von diesen sind aber sechs zu verwerfen, nämlich $(\pm 13, 1, \mp 6)$, $(\pm 14, 3, \mp 5)$, $(\pm 15, 2, \mp 5)$; die übrigen zweiunddreissig umfassen sämtliche reducierten Formen. Nach der zweiten Methode ergeben sich dieselben Formen in folgender Reihenfolge*).

$$(\pm 7, 3, \mp 10), (\pm 10, 3, \mp 7), (\pm 7, 4, \mp 9), (\pm 9, 4, \mp 7), (\pm 6, 5, \mp 9),$$
$$(\pm 9, 5, \mp 6), (\pm 2, 7, \mp 15), (\pm 3, 7, \mp 10), (\pm 5, 7, \mp 6), (\pm 6, 7, \mp 5),$$
$$(\pm 10, 7, \mp 3), (\pm 15, 7, \mp 2), (\pm 1, 8, \mp 15), (\pm 3, 8, \mp 5), (\pm 5, 8, \mp 3),$$
$$(\pm 15, 8, \mp 1).$$

186.

Es sei F eine reducierte Form mit der Determinante D und dieser sei nach rechts hin die reducierte Form F', dieser wieder nach rechts hin die reducierte Form F'', dieser nach rechts hin die reducierte Form F''' u. s. w. benachbart. Dann sind offenbar sämtliche Formen F', F'', F''', ... vollständig bestimmt und sowohl unter einander als auch der Form F eigentlich äquivalent. Da aber die Anzahl aller reducierten Formen mit gegebener Determinante eine endliche ist, so ist klar, dass nicht alle Formen in der unendlichen Reihe F, F', F'', ... von einander verschieden sein können. Nehmen wir $F^{(m)}$ und $F^{(m+n)}$ als identisch an, so werden $F^{(m-1)}$ und $F^{(m+n-1)}$

*) Für $b = 1$ lässt sich -78 nicht in zwei Factoren zerlegen, die ohne Rücksicht auf das Vorzeichen zwischen $\sqrt{79} + 1$, und $\sqrt{79} - 1$ liegen; daher ist dieser Wert und aus demselben Grunde auch die Werte 2 und 6 zu verwerfen.

reduciert, derselben reducierten Form nach links hin benachbart und daher identisch sein; somit werden ebenso $F^{(m-2)}$ und $F^{(m+n-2)}$ u. s. w., schliesslich F und $F^{(n)}$ identisch sein. Daher wird in der Reihe $F, F', F'', \ldots$, wenn sie nur weit genug fortgesetzt wird, notwendig einmal die erste Form F wiederkehren, und wenn wir annehmen, dass $F^{(n)}$ die erste mit F identische Form ist, oder dass alle $F', F'', \ldots, F^{(n-1)}$ von F verschieden seien, so ist leicht ersichtlich, dass alle $F, F', F'', \ldots, F^{(n-1)}$ von einander verschieden sind. Den Complex dieser Formen nennen wir die **Periode der Form** F. Wenn daher die Reihe über die letzte Form der Periode hinaus fortgesetzt wird, so werden dieselben Formen $F, F', F'', \ldots$ immer von Neuem entstehen und die ganze unendliche Reihe wird aus dieser unendlich oftmal wiederholten Periode der Form F gebildet sein.

Die Reihe $F, F', F'', \ldots$ kann auch rückwärts fortgesetzt werden, indem man der Form F die reducierte Form $'F$, welche ihr nach links hin benachbart ist, dieser wiederum die reducierte Form $''F$, welche ihr nach links hin benachbart ist, u. s. w. vorsetzt. Man erhält auf diese Weise die nach beiden Seiten unendliche Reihe von Formen

$$\ldots, \; '''F, \; ''F, \; 'F, \; F, \; F', \; F'', \; F''', \; \ldots$$

und sieht leicht, dass $'F$ mit $F^{(n-1)}$, $''F$ mit $F^{(n-2)}$ u. s. w. identisch ist und somit die Reihe auch nach links hin aus der unendlich oftmal wiederholten Periode der Form F besteht.

Wenn man den Formen $F, F', F'', \ldots, 'F, ''F, \ldots$ die Indices $0, 1, 2, \ldots, -1, -2, \ldots$ respective und allgemein der Form $F^{(m)}$ den Index m, der Form $^{(m)}F$ den Index $-m$ beilegt, so werden offenbar irgend zwei Formen der Reihe identisch oder verschieden sein, je nachdem die Indices derselben nach dem Modul n congruent oder incongruent sind.

Beispiel. Als Periode der Form $(3, 8, -5)$, deren Determinante gleich 79 ist, findet sich die folgende: $(3, 8, -5)$, $(-5, 7, 6)$, $(6, 5, -9)$, $(-9, 4, 7)$, $(7, 3, -10)$, $(-10, 7, 3)$. Nach der letzten Form ergiebt sich wiederum $(3, 8, -5)$. Hier ist also $n = 6$.

187.

Im Folgenden geben wir einige allgemeine Bemerkungen über diese Perioden.

1. Wenn die Formen $F, F', F'', \ldots, 'F, ''F, '''F, \ldots$ folgendermassen dargestellt werden:

$$(a, b, -a'), \; (-a', b', a''), \; (a'', b'', -a'''), \ldots, \; (-'a, 'b, a), \; (''a, ''b, -'a), \; (-'''a, '''b, ''a), \ldots,$$

so werden alle Grössen $a, a', a'', a''', \ldots, 'a, ''a, '''a, \ldots$ dasselbe Vorzeichen haben (Artikel 184, 1), alle $b, b', b'', \ldots, 'b, ''b, \ldots$ aber werden positiv sein.

2. Hieraus geht hervor, dass die Zahl n (die Anzahl der Formen, aus denen die Periode der Form F besteht) stets gerade ist. Denn das erste Glied irgend einer Form $F^{(m)}$ aus dieser Periode wird offenbar dasselbe Vorzeichen besitzen, wie das erste Glied a der Form F, wenn m gerade, das entgegengesetzte aber, wenn m ungerade ist. Somit wird, da $F^{(n)}$ und F identisch sind, n notwendig gerade sein.

3. Der Algorithmus, durch welchen die Zahlen b', b'', b''', ..., a'', a''', ... gefunden werden, ist nach Artikel 184, 6 folgender:

$$b' \equiv -b \pmod{a'} \text{ zwischen den Grenzen } \sqrt{D} \text{ und } \sqrt{D} \mp a'; \quad a'' = \frac{D-b'^2}{a'}$$

$$b'' \equiv -b' \pmod{a''} \ldots\ldots\ldots \sqrt{D} \text{ und } \sqrt{D} \mp a''; \quad a''' = \frac{D-b''^2}{a''}$$

$$b''' \equiv -b'' \pmod{a'''} \ldots\ldots\ldots \sqrt{D} \text{ und } \sqrt{D} \mp a'''; \quad a'''' = \frac{D-b'''^2}{a'''}$$

u. s. w.,

wobei in der zweiten Kolonne die oberen oder unteren Zeichen zu nehmen sind, je nachdem a, a', a'', ... positiv oder negativ sind. Anstatt der Formeln in der dritten Kolonne können auch die folgenden genommen werden, welche bequemer sind, falls D eine grosse Zahl ist:

$$a'' = \frac{b+b'}{a'}(b-b') + a$$

$$a''' = \frac{b'+b''}{a''}(b'-b'') + a'$$

$$a'''' = \frac{b''+b'''}{a'''}(b''-b''') + a''$$

u. s. w.

4. Jede Form $F^{(m)}$, welche in der Periode der Form F enthalten ist, wird im Wesentlichen dieselbe Periode haben wie F. Jene Periode wird nämlich sein: $F^{(m)}$, $F^{(m+1)}$, ..., $F^{(n-1)}$, F, F', ..., $F^{(m-1)}$, und in dieser kommen dieselben Formen und in derselben Reihenfolge vor, wie in der Periode der Form F, und sie unterscheidet sich von letzterer nur in Bezug auf den Anfang und das Ende.

5. Hieraus folgt, dass alle reducierten Formen mit derselben Determinante D in Perioden verteilt werden können. Man nehme nach Belieben irgend eine dieser Formen F und suche deren Periode F, F', F'', ..., $F^{(n-1)}$, die mit P bezeichnet sein möge. Wenn diese noch nicht alle reducierten Formen mit der Determinante D umfasst, so sei irgend eine in ihr nicht enthaltene Form G und Q die Periode dieser. Dann ist klar, dass P und Q keine Form gemeinschaftlich haben können, denn sonst würde G auch in P enthalten sein müssen und die Perioden würden überhaupt zusammenfallen. Wenn P und Q noch nicht alle reducierten Formen erschöpfen, so wird eine der nicht darin vorkommenden

H eine dritte Periode R ergeben, welche weder mit P noch mit Q eine Form gemeinsam hat. Auf diese Weise kann man fortfahren, bis alle reducierten Formen erschöpft sind. So verteilen sich z. B. alle reducierten Formen mit der Determinante 79 auf sechs Perioden:

I. (1, 8, — 15), (— 15, 7, 2), (2, 7, — 15), (— 15, 8, 1).
II. (— 1, 8, 15), (15, 7, — 2), (— 2, 7, 15), (15, 8, — 1).
III. (3, 8, — 5), (— 5, 7, 6), (6, 5, — 9), (— 9, 4, 7), (7, 3, — 10), (— 10, 7, 3).
IV. (— 3, 8, 5), (5, 7, — 6), (— 6, 5, 9), (9, 4, — 7), (— 7, 3, 10), (10, 7, — 3).
V. (5, 8, — 3), (— 3, 7, 10), (10, 3, — 7), (— 7, 4, 9), (9, 5, — 6), (— 6, 7, 5).
VI. (— 5, 8, 3), (3, 7, — 10), (— 10, 3, 7), (7, 4, — 9), (— 9, 5, 6), (6, 7, — 5).

6) Wir werden **associierte Formen** solche Formen nennen, welche aus denselben aber in umgekehrter Reihenfolge stehenden Gliedern bestehen, z. B. $(a, b, -a')$, $(-a', b, a)$. Dann ist aus Artikel 184,7 leicht ersichtlich, dass, wenn die reducierte Form F die Periode hat $F, F', F'', \ldots, F^{(n-1)}$, ferner der Form F die Form f und den Formen $F^{(n-1)}, F^{(n-2)}, \ldots, F'', F'$ respective die Formen $f', f'', \ldots, f^{(n-2)}, f^{(n-1)}$ associiert sind, die Periode der Form f die folgende ist $f, f', f'', \ldots, f^{(n-2)}, f^{(n-1)}$ und somit aus ebenso vielen Formen besteht, wie die Periode der Form F. Die Perioden associierter Formen werden wir **associierte Perioden** nennen. So sind in unserm Beispiel die Perioden III und VI und ebenso IV und V associiert.

7). Es ist aber auch möglich, dass die Form f selbst in der ihr associierten Form F vorkommt, wie in unserm Beispiel in der Periode I und II, und dass somit die Periode der Form F mit der Periode der Form f übereinstimmt oder dass die Periode der Form F **sich selbst associiert** ist. So oft dies der Fall ist, kommen in dieser Periode zwei ambige Formen vor. Nehmen wir nämlich an, dass die Periode der Form F aus $2n$ Formen bestehe oder dass F und $F^{(2n)}$ identisch seien, und ist ferner $2m+1$ der Index der Form f in der Periode der Form F*) oder sind $F^{(2m+1)}$ und F associiert, so sind offenbar auch F' und $F^{(2m)}$, ebenso F'' und $F^{(2m-1)}$ u. s. w. und daher auch $F^{(m)}$ und $F^{(m+1)}$ associiert. Ist $F^{(m)} = (a^{(m)}, b^{(m)}, -a^{(m+1)})$, $F^{(m+1)} = (-a^{(m+1)}, b^{(m+1)}, a^{(m+2)})$, so wird $b^{(m)} + b^{(m+1)} \equiv 0 \pmod{a^{(m+1)}}$; nach der Erklärung der associierten Formen ist aber $b^{(m)} = b^{(m+1)}$ und somit $2b^{(m+1)} \equiv 0 \pmod{a^{(m+1)}}$, oder die Form $F^{(m+1)}$ ist ambig. — Ebenso sind $F^{(2m+1)}$ und $F^{(2n)}$, somit auch $F^{(2m+2)}$ und $F^{(2n-1)}$, ferner $F^{(2m+3)}$ und $F^{(2n-2)}$ u. s. w. und schliesslich $F^{(m+n)}$ und $F^{(m+n+1)}$ associiert; von diesen ist aber die letztere ambig, wie durch ähnliche Schlüsse leicht bewiesen wird. Da aber $m+1$ und $m+n+1$ nach dem Modul $2n$ incongruent

*) Der Index ist hier notwendig ungerade, weil offenbar die ersten Glieder der Formen F, f entgegengesetzte Zeichen haben. (Vgl. oben unter 2).

sind, so sind die Formen $F^{(m+1)}$ und $F^{(m+n+1)}$ nicht identisch (Artikel 186, wo n dasselbe bezeichnet, wie hier $2n$). So finden sich in I die ambigen Formen (1, 8, — 15), (2, 7, — 15), in II die Formen (— 1, 8, 15), (— 2, 7, 15).

8. Umgekehrt ist jede Periode, in welcher eine ambige Form vorkommt, sich selbst associiert. Denn man sieht leicht, dass, wenn $F^{(m)}$ eine ambige reducierte Form ist, die ihr associierte Form (welche ebenfalls reduciert ist) ihr zugleich nach links hin benachbart ist, d. h. dass $F^{(m-1)}$ und $F^{(m)}$ associiert sind. Dann ist aber die ganze Periode sich selbst associiert. — Hieraus geht hervor, dass es nicht möglich ist, dass nur eine einzige ambige Form in irgend einer Periode enthalten ist.

9. Es können aber auch nicht mehr wie zwei in derselben Periode vorkommen. Nehmen wir nämlich an, dass es in der aus $2n$ Formen bestehenden Periode der Form F drei ambige Formen $F^{(\lambda)}$, $F^{(\mu)}$, $F^{(\nu)}$ gebe, welche respective zu den Indices λ, μ, ν gehören, so dass λ, μ, ν ungleiche zwischen den Grenzen 0 und $2n - 1$ (einschliesslich) liegende Zahlen sind, so sind die Formen $F^{(\lambda-1)}$ und $F^{(\lambda)}$ und ebenso $F^{(\lambda-2)}$ und $F^{(\lambda+1)}$ u. s. w. und schliesslich F und $F^{(2\lambda-1)}$ associiert. Aus demselben Grunde sind F und $F^{(2\mu-1)}$ sowie auch F und $F^{(2\nu-1)}$ associiert. Demnach sind $F^{(2\lambda-1)}$, $F^{(2\mu-1)}$, $F^{(2\nu-1)}$ identisch und die Indices $2\lambda - 1$, $2\mu - 1$, $2\nu - 1$ sind nach dem Modul $2n$ congruent, mithin auch $\lambda \equiv \mu \equiv \nu \pmod{n}$. Dies ist aber absurd, weil offenbar zwischen den Grenzen 0 und $2n - 1$ drei verschiedene nach dem Modul n congruente Zahlen nicht liegen können.

188.

Da alle Formen aus derselben Periode eigentlich äquivalent sind, so entsteht die Frage, ob nicht auch Formen aus verschiedenen Perioden eigentlich äquivalent sein können. Bevor wir aber zeigen, dass dies unmöglich ist, müssen wir Einiges über die Transformation reducierter Formen auseinandersetzen.

Da wir im Folgenden sehr häufig von der Transformation der Formen handeln müssen, so werden wir uns, um Weitläufigkeiten soviel wie möglich zu vermeiden, von hier ab stets der folgenden abgekürzten Schreibweise bedienen. Wenn die Form $LX^2 + 2MXY + NY^2$ durch die Substitution $X = \alpha x + \beta y$, $Y = \gamma x + \delta y$ in die Form $lx^2 + 2mxy + ny^2$ transformiert wird, so werden wir einfach sagen, (L, M, N) gehe durch die Substitution $\alpha, \beta, \gamma, \delta$ in (l, m, n) über. Auf diese Weise wird es nicht nötig sein, die Unbestimmten der einzelnen in Rede stehenden Formen besonders zu bezeichnen. — Offenbar aber muss die erste Unbestimmte von der zweiten in jeder Form wohl unterschieden werden.

Gegeben sei die reducierte Form $(a, b, -a')$ oder f mit der Determinante D. Man bilde in analoger Weise wie im Artikel 186 die nach beiden

Seiten ins Unendliche gehende Reihe reducierter Formen ..., $''f, 'f, f, f', f'', \ldots$, und zwar sei:

$$f' = (-a', b', a''), \quad f'' = (a'', b'', -a'''), \ldots$$
$$'f = (-'a, 'b, a), \quad ''f = (''a, ''b, -'a), \ldots$$

Setzt man

$$\frac{b+b'}{-a'} = h', \quad \frac{b'+b''}{a''} = h'', \quad \frac{b''+b'''}{-a'''} = h''', \ldots$$
$$\frac{'b+b}{a} = h, \quad \frac{''b+'b}{-'a} = 'h, \quad \frac{'''b+''b}{''a} = ''h, \ldots,$$

so wird offenbar, wenn man (wie in Artikel 177) die Zahlen $\alpha', \alpha'', \alpha''', \ldots, \beta', \beta'', \beta''', \ldots$ u. s. w. nach folgendem Algorithmus bildet:

$$\begin{array}{llll} \alpha' = 0, & \beta' = -1, & \gamma' = 1, & \delta' = h' \\ \alpha'' = \beta', & \beta'' = h''\,\beta', & \gamma'' = \delta', & \delta'' = h''\,\delta' - 1 \\ \alpha''' = \beta'', & \beta''' = h'''\,\beta'' - \beta', & \gamma''' = \delta'', & \delta''' = h'''\,\delta'' - \delta' \\ \alpha'''' = \beta''', & \beta'''' = h''''\beta''' - \beta'', & \gamma'''' = \delta''', & \delta'''' = h''''\delta''' - \delta'' \end{array}$$

u. s. w.,

f transformiert werden in

f' durch die Substitution $\alpha', \beta', \gamma', \delta'$
f'' „ „ „ $\alpha'', \beta'', \gamma'', \delta''$
f''' „ „ „ $\alpha''', \beta''', \gamma''', \delta'''$
u. s. w.,

und alle diese Transformationen werden eigentliche sein.

Da $'f$ in f übergeht durch die eigentliche Substitution $0, -1, 1, h$ (Artikel 158), so wird f in $'f$ durch die eigentliche Substitution $h, 1, -1, 0$ übergehen. Aus analogem Grunde wird $'f$ in $''f$ durch die eigentliche Substitution $'h, 1, -1, 0$, $''f$ in $'''f$ durch die eigentliche Substitution $''h, 1, -1, 0$ übergehen u. s. w. Hieraus folgt gemäss Artikel 159 in derselben Weise wie im Artikel 177, dass, wenn die Zahlen $'\alpha, ''\alpha, '''\alpha, \ldots, '\beta, ''\beta, '''\beta, \ldots$ u. s. w. nach folgendem Algorithmus gebildet werden:

$$\begin{array}{llll} '\alpha = h, & '\beta = 1, & '\gamma = -1, & '\delta = 0 \\ ''\alpha = 'h\,'\alpha - 1, & ''\beta = '\alpha, & ''\gamma = 'h\,'\gamma, & ''\delta = '\gamma \\ '''\alpha = ''h\,''\alpha - '\alpha, & '''\beta = ''\alpha, & '''\gamma = ''h\,''\gamma - '\gamma, & '''\delta = ''\gamma \\ ''''\alpha = '''h'''\alpha - ''\alpha, & ''''\beta = '''\alpha, & ''''\gamma = '''h'''\gamma - ''\gamma, & ''''\delta = '''\gamma \end{array}$$

u. s. w.,

f übergeht in

$'f$ durch die Substitution $'\alpha, '\beta, '\gamma, '\delta$
$''f$ „ „ „ $''\alpha, ''\beta, ''\gamma, ''\delta$
$'''f$ „ „ „ $'''\alpha, '''\beta, '''\gamma, '''\delta$
u. s. w.,

und dass alle diese Transformationen eigentliche sind.

Setzt man $\alpha = 1, \beta = 0, \delta = 1$, so werden diese Zahlen zur Form f dieselbe Beziehung haben, wie $\alpha', \beta', \gamma', \delta'$ zu f'; $\alpha'', \beta'', \gamma'', \delta''$ zu

f'' u. s. w., $'\alpha$, $'\beta$, $'\gamma$, $'\delta$ zu $'f$ u. s. w. Durch die Substitution α, β, γ, δ nämlich geht die Form f in f über. Dann aber werden die unendlichen Reihen α', α'', α''', ..., $'\alpha$, $''\alpha$, $'''\alpha$, ... durch Einschiebung des Gliedes α in so enge Verbindung gebracht, dass man sie sich als eine einzige zusammenhängende nach beiden Seiten unendliche Reihe denken kann, welche überall nach demselben Gesetz fortschreitet: ..., $'''\alpha$, $''\alpha$, $'\alpha$, α, α', α'', α''', ... Das Fortschreitungsgesetz ist folgendes:

$$'''\alpha + '\alpha = ''h''\alpha,\ ''\alpha + \alpha = 'h'\alpha,\ '\alpha + \alpha' = h\alpha,\ \alpha + \alpha'' = h'\alpha',\ \alpha' + \alpha''' = h''\alpha'', \ldots,$$

oder allgemein (wenn man annimmt, dass ein negativer rechts angefügter Index dasselbe bezeichnet, wie ein positiver links angefügter):

$$\alpha^{(m-1)} + \alpha^{(m+1)} = h^{(m)}\alpha^{(m)}.$$

Analog ist die Reihe ..., $''\beta$, $'\beta$, β, β', β'', ... eine stetig zusammenhängende, deren Gesetz ist:

$$\beta^{(m-1)} + \beta^{(m+1)} = h^{(m+1)}\beta^{(m)},$$

und diese wird mit der vorhergehenden identisch sein, wenn man alle Glieder um eine Stelle vorrückt, $''\beta = '\alpha$, $'\beta = \alpha$, $\beta = \alpha'$, u. s. w. Das Gesetz der continuierlichen Reihe ..., $''\gamma$, $'\gamma$, γ, γ', γ'', ... ist folgendes:

$$\gamma^{(m-1)} + \gamma^{(m+1)} = h^{(m)}\gamma^{(m)},$$

uud das Gesetz der Reihe ..., $''\delta$, $'\delta$, δ, δ', δ'', ... ist:

$$\delta^{(m-1)} + \delta^{(m+1)} = h^{(m+1)}\delta^{(m)},$$

und überdies ist allgemein $\delta^{(m)} = \gamma^{(m+1)}$.

Beispiel. Ist die gegebene Form f die folgende (3, 8, —5), so wird dieselbe transformiert

i. d. Form	${}'''''''f$	od. (—10, 7, 3)	durch d. Subst.:	—805, —152, +143, +27
„	${}''''''f$	„ (3, 8, —5)	„ „ „	—152, +45, +27, —8
„	${}'''''f$	„ (—5, 7, 6)	„ „ „	+45, +17, —8, —3
„	${}''''f$	„ (6, 5, —9)	„ „ „	+17, —11, —3, +2
„	${}'''f$	„ (—9, 4, 7)	„ „ „	—11, —6, +2, +1
„	${}''f$	„ (7, 3, —10)	„ „ „	—6, +5, +1, —1
„	${}'f$	„ (—10, 7, 3)	„ „ „	+5, +1, —1, 0
„	f	„ (3, 8, —5)	„ „ „	+1, 0, 0, +1
„	f'	„ (—5, 7, 6)	„ „ „	0, —1, +1, —3
„	f''	„ (6, 5, —9)	„ „ „	—1, —2, —3, —7
„	f'''	„ (—9, 4, 7)	„ „ „	—2, +3, —7, +10
„	f''''	„ (7, 3, —10)	„ „ „	+3, +5, +10, +17
„	f'''''	„ (—10, 7, 3)	„ „ „	+5, —8, +17, —27
„	f''''''	„ (3, 8, —5)	„ „ „	—8, —45, —27, —152
„	f'''''''	„ (—5, 7, 6)	„ „ „	—45, +143, —152, +483

u. s. w.

189.

In Betreff dieses Algorithmus ist Folgendes anzumerken.

1. Alle Zahlen a, a' a'', ..., $'a$, $''a$, ... haben dasselbe Vorzeichen; alle Zahlen b, b', b'', ..., $'b$, $''b$, ... sind positiv. In der Reihe ... $''h$, $'h$, h, h', h'', ... wechseln die Vorzeichen ab; es wird nämlich, falls sämtliche Zahlen a, a', ... positiv sind, $h^{(m)}$ oder $^{(m)}h$ positiv sein für ein gerades m, negativ für ein ungerades m; wenn aber a, a', ... negativ sind, so wird $h^{(m)}$ oder $^{(m)}h$ negativ bei geradem m und positiv bei ungeradem m.

2. Wenn a positiv und daher h' negativ, h'' positiv u. s. w. ist, so ist $\alpha'' = -1$ negativ, $\alpha''' = h''\alpha''$ negativ und grösser als α'' (oder gleich α'', wenn $h'' = 1$ ist); $\alpha'''' = h'''\alpha''' - \alpha''$ positiv und grösser als α''' (weil $h'''\alpha'''$ positiv, α'' negativ ist); $\alpha''''' = h''''\alpha'''' - \alpha'''$ positiv und grösser als α'''' (weil $h''''\alpha''''$ positiv ist) u. s. w. Hieraus folgt leicht, dass die Reihe α', α'', α''' ... ins Unendliche wächst und dass immer zwei positive Zeichen mit zwei negativen abwechseln, so dass $\alpha^{(m)}$ das Zeichen $+$, $+$, $-$, $-$ hat, je nachdem $m \equiv 0, 1, 2, 3 \pmod{4}$ ist. — Ist a negativ, so findet man durch eine ähnliche Schlussreihe α'' negativ, α''' positiv und entweder grösser als α'' oder gleich α''; α'''' positiv und grösser als α'''; α''''' negativ und grösser als α'''' u. s. w., so dass die Reihe α', α'', α''', ... fortwährend wächst und das Zeichen des Gliedes $\alpha^{(m)}$ $+$, $-$, $-$, $+$ ist, je nachdem $m \equiv 0, 1, 2, 3 \pmod{4}$ ist.

3. Auf diese Weise findet man, dass alle vier unendlichen Reihen α', α'', α''', ..., γ, γ', γ'', ..., α', α, $'\alpha$, $''\alpha$, ..., γ, $'\gamma$, $''\gamma$, ... und somit auch die folgenden mit jenen identischen Reihen β, β', β'', ..., $'\delta$, δ, δ', δ'', ..., β, $'\beta$, $''\beta$, ..., $'\delta$, $''\delta$, ... beständig wachsen und, je nachdem $m \equiv 0, 1, 2, 3 \pmod{4}$ ist, das Zeichen

von $\alpha^{(m)}$ $+, \pm, -, \mp$, von $\beta^{(m)}$ $\pm, -, \mp, +$
von $\gamma^{(m)}$ $\pm, +, \mp, -$, von $\delta^{(m)}$ $+, \mp, -, \pm$
von $^{(m)}\alpha$ $+, \pm, -, \mp$, von $^{(m)}\beta$ $\mp, +, \pm, -$
von $^{(m)}\gamma$ $\mp, -, \pm, +$, von $^{(m)}\delta$ $+, \mp, -, \pm$

ist, wo die oberen Zeichen gelten, falls a positiv, die unteren, falls a negativ ist. Besonders aber möge man sich folgende Eigenschaft merken: Bezeichnet m irgend einen positiven Index, so werden $\alpha^{(m)}$ und $\gamma^{(m)}$ dasselbe Zeichen haben, wenn a positiv, dagegen entgegengesetztes, wenn a negativ ist, und analog $\beta^{(m)}$ und $\delta^{(m)}$; dagegen werden $^{(m)}\alpha$ und $^{(m)}\gamma$ oder $^{(m)}\beta$ oder $^{(m)}\delta$ dasselbe Zeichen haben, wenn a negativ, und entgegengesetztes, wenn a positiv ist.

4. In der Bezeichnung des Artikels 27 lässt sich die Grösse von $\alpha^{(m)}$, ... kurz folgendermassen ausdrücken. Setzt man

$$\mp h' = k', \ \pm h'' = k'', \ \mp h''' = k''', \ \ldots, \ \pm h = k, \ \mp {}'h = {}'k, \ \pm {}''h = {}''k, \ldots,$$

so dass sämtliche k', k'', ..., k, $'k$, ... positive Zahlen sind, so ist:

$$\alpha^{(m)} = \pm[k'', k''', k'''', \ldots, k^{(m-1)}]; \quad \beta^{(m)} = \pm[k'', k''', k'''', \ldots, k^{(m)}]$$
$$\gamma^{(m)} = \pm[k', k'', k''', \ldots, k^{(m-1)}]; \quad \delta^{(m)} = \pm[k', k'', k''', \ldots, k^{(m)}]$$
$$^{(m)}\alpha = \pm[k, 'k, ''k, \ldots, {}^{(m-1)}k]; \quad ^{(m)}\beta = \pm[k, 'k, ''k, \ldots, {}^{(m-2)}k]$$
$$^{(m)}\gamma = \pm['k, ''k, '''k, \ldots, {}^{(m-1)}k]; \quad ^{(m)}\delta = \pm['k, ''k, '''k, \ldots, {}^{(m-2)}k],$$

wobei die Vorzeichen nach den oben angeführten Regeln bestimmt werden müssen. Nach diesen Formeln, deren Beweis wir seiner Leichtigkeit wegen weglassen, kann die Rechnung stets auf die kürzeste Weise durchgeführt werden.

190.

Hülfssatz. Bezeichnen m, μ, m', n, ν, n' irgend welche ganze Zahlen, derart jedoch, dass von den drei letzteren keine gleich Null ist, so behaupte ich, dass, wenn $\frac{\mu}{\nu}$ zwischen den Grenzen $\frac{m}{n}$ und $\frac{m'}{n'}$ (diese ausgeschlossen) liegt und $mn' - nm' = \pm 1$ ist, der Nenner ν grösser sein wird als n und n'.

Beweis. Offenbar liegt $\mu nn'$ zwischen $\nu mn'$ und $\nu nm'$ und unterscheidet sich daher von beiden Grenzen um weniger als die eine Grenze von der andern, d. h. es wird $\nu mn' - \nu nm' > \mu nn' - \nu mn'$ und $> \mu nn' - \nu nm'$ oder $\nu > n'(\mu n - \nu m)$ und $> n(\mu n' - \nu m')$ sein. Hieraus folgt, dass, da $\mu n - \nu m$ sicher nicht gleich Null $\left(\text{denn sonst würde im Widerspruch mit der Voraussetzung } \frac{\mu}{\nu} = \frac{m}{n} \text{ sein}\right)$ und auch $\mu n' - \nu m'$ nicht gleich Null (aus ähnlichem Grunde), vielmehr jeder der beiden Ausdrücke gleich 1 ist, $\nu > n'$ und $> n$ ist.

Es ist daher klar, dass ν nicht gleich 1 sein kann, d. h., wenn $mn' - nm' = \pm$ ist, dass zwischen den Brüchen $\frac{m}{n}$, $\frac{m'}{n'}$ keine ganze Zahl liegen kann. Daher kann auch nicht die Null zwischen ihnen liegen, d. h. jene Brüche können nicht entgegengesetzte Zeichen haben.

191.

Satz. Wenn die reducierte Form $(a, b, -a')$ mit der Determinante D durch die Substitution α, β, γ, δ in die reducierte Form $(A, B, -A')$ mit derselben Determinante übergeht, so liegt erstens $\frac{\pm\sqrt{D} - b}{a}$ zwischen $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$ (wenn nämlich weder γ noch δ gleich Null ist, d. h. wenn beide Grenzen endlich sind), wobei das obere Zeichen zu nehmen ist, wenn keine von beiden Grenzen das dem Zeichen von a entgegengesetzte Zeichen hat

(oder deutlicher, wenn entweder beide Grenzen dasselbe Zeichen haben wie a oder die eine dasselbe Zeichen hat wie a, die andere aber gleich Null ist); das untere aber, wenn keine der beiden Grenzen dasselbe Zeichen hat wie a; — zweitens $\frac{\pm\sqrt{D}+b}{a'}$ zwischen $\frac{\gamma}{\alpha}$ und $\frac{\delta}{\beta}$ (wenn nämlich weder α noch β gleich Null ist), wo das obere Zeichen gilt, wenn keine der beiden Grenzen das dem Vorzeichen von a' (oder a) entgegengesetzte Vorzeichen hat, das untere, wenn keine derselben dasselbe Zeichen hat wie a'*).

Beweis. Man hat die Gleichungen:

[1] $$a\alpha^2 + 2b\alpha\gamma - a'\gamma^2 = A$$

[2] $$a\beta^2 + 2b\beta\delta - a'\delta^2 = -A'.$$

Aus diesen folgt:

[3] $$\frac{\alpha}{\gamma} = \frac{\pm\sqrt{D + \frac{aA}{\gamma^2}} - b}{a}$$

[4] $$\frac{\beta}{\delta} = \frac{\pm\sqrt{D - \frac{aA'}{\delta^2}} - b}{a}$$

[5] $$\frac{\gamma}{\alpha} = \frac{\pm\sqrt{D - \frac{a'A'}{\alpha^2}} + b}{a'}$$

[6] $$\frac{\delta}{\beta} = \frac{\pm\sqrt{D + \frac{a'A'}{\beta^2}} + b}{a'}.$$

Die Gleichung [3], [4], [5], [6] ist wegzulassen, wenn respective γ, δ, α, β, gleich Null ist. — Doch bleibt es hier zweifelhaft, welche Vorzeichen den Wurzelgrössen zugelegt werden müssen. Dies entscheiden wir in folgender Weise.

Es ist sofort klar, dass in [3] und [4] notwendig die oberen Zeichen genommen werden müssen, wenn weder $\frac{\alpha}{\gamma}$ noch $\frac{\beta}{\delta}$ das dem Vorzeichen von a entgegengesetzte Zeichen hat, weil, wenn man das untere Zeichen nähme, $\frac{a\alpha}{\gamma}$ und $\frac{a\beta}{\delta}$ negative Grössen werden würden. Weil aber A und A' die-

*) Offenbar können andere Fälle nicht stattfinden, da dem vorigen Artikel zufolge wegen $\alpha\delta - \beta\gamma = \pm 1$ beide Grenzen weder entgegengesetzte Zeichen haben noch gleichzeitig gleich Null sein können.

selben Zeichen haben, so fällt $\sqrt{D}$ zwischen $\sqrt{D+\frac{aA}{\gamma^2}}$ und $\sqrt{D-\frac{aA'}{\delta^2}}$, und daher liegt in diesem Falle $\frac{\sqrt{D}-b}{a}$ zwischen $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$. Somit ist der erste Teil unseres Satzes für den ersteren Fall bewiesen.

Auf dieselbe Weise erkennt man, dass in [5] und [6] notwendig die unteren Zeichen genommen werden müssen, wenn weder $\frac{\gamma}{\alpha}$ noch $\frac{\delta}{\beta}$ dasselbe Zeichen hat wie a' oder a, weil, wenn das obere Zeichen genommen würde, $\frac{a'\gamma}{\alpha}$ und $\frac{a'\delta}{\beta}$ notwendig positive Grössen werden würden. Hieraus folgt sogleich, dass $\frac{-\sqrt{D}+b}{a'}$ für diesen Fall zwischen $\frac{\gamma}{\alpha}$ und $\frac{\delta}{\beta}$ liegt. Es ist daher auch der zweite Teil des Satzes für den letzten Fall bewiesen. Wenn nun ebenso leicht gezeigt werden könnte, dass in [3] und [4] die unteren Zeichen genommen werden müssen, wenn keine der beiden Grössen $\frac{\alpha}{\gamma}$, $\frac{\beta}{\delta}$ dasselbe Zeichen hat wie a, und in [5] und [6] die oberen, wenn weder $\frac{\gamma}{\alpha}$ noch $\frac{\delta}{\beta}$ entgegengesetztes Zeichen hat wie a, so würde hieraus in ähnlicher Weise folgen, dass für jenen Fall $\frac{-\sqrt{D}-b}{a}$ zwischen $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$, für diesen $\frac{\sqrt{D}+b}{a'}$ zwischen $\frac{\gamma}{\alpha}$ und $\frac{\delta}{\beta}$ liegt, oder es würde der erste Teil des Satzes auch für den letzten Fall und der zweite Teil desselben auch für den ersten Fall bewiesen sein. Obwohl aber jenes nicht schwierig ist, lässt es sich doch nicht ohne einige Umschweife abmachen und ziehen wir daher die folgende Methode vor.

Wenn keine der Zahlen α, β, γ, δ gleich Null ist, werden $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$ dieselben Vorzeichen haben wie $\frac{\gamma}{\alpha}$ und $\frac{\delta}{\beta}$. Wenn daher keine dieser beiden Grössen dasselbe Zeichen hat wie a' oder a, und daher $\frac{-\sqrt{D}+b}{a'}$ zwischen $\frac{\gamma}{\alpha}$ und $\frac{\delta}{\beta}$ fällt, so wird keine der beiden Grössen $\frac{\alpha}{\gamma}$, $\frac{\beta}{\delta}$ dasselbe Zeichen wie a haben und daher $\frac{a'}{-\sqrt{D}+b}=\frac{-\sqrt{D}-b}{a}$ (wegen $aa'=D-b^2$) zwischen $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$ fallen. Demnach ist für denjenigen Fall, wo weder $\alpha=0$ noch $\beta=0$ ist, der erste Teil des Satzes auch für den zweiten Fall bewiesen (denn die Bedingung, dass weder $\gamma=0$ noch $\delta=0$ sei, ist schon im Satze selbst hinzugefügt). In analoger Weise wird, wenn keine der

Zahlen α, β, γ, δ gleich Null ist und weder $\frac{\alpha}{\gamma}$ noch $\frac{\beta}{\delta}$ das dem Vorzeichen von a oder a' entgegengesetzte Zeichen hat und daher $\frac{\sqrt{D}-b}{a}$ zwischen $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$ liegt, auch $\frac{\gamma}{\alpha}$ und $\frac{\delta}{\beta}$ kein dem Vorzeichen von a' entgegengesetztes Vorzeichen haben und daher $\frac{a}{\sqrt{D}-b} = \frac{\sqrt{D}+b}{a'}$ zwischen $\frac{\gamma}{\alpha}$ und $\frac{\delta}{\beta}$ fallen. In demjenigen Falle also, wo weder $\gamma = 0$ noch $\delta = 0$ ist, ist der zweite Teil des Satzes auch für den zweiten Fall bewiesen.

Es bleibt daher nur noch zu beweisen übrig, dass der erste Teil des Satzes auch für den zweiten Fall stattfindet, wenn eine der beiden Zahlen α, β gleich Null ist, und dass der zweite Teil des Satzes auch für den ersten Fall gilt, wenn entweder $\gamma = 0$ oder $\delta = 0$ ist. Alle diese Fälle aber sind unmöglich. Denn nehmen wir an, für den ersten Teil des Satzes, dass weder $\gamma = 0$ noch $\delta = 0$ sei, dass $\frac{\alpha}{\beta}$, $\frac{\beta}{\delta}$ nicht dasselbe Zeichen haben wie a und dass

1. $\alpha = 0$ sei. Dann folgt aus der Gleichung $\alpha\delta - \beta\gamma = \pm 1$, dass $\beta = \pm 1$, $\gamma = \pm 1$ ist. Hiernach ist, der Gleichung [1] zufolge, $A = -a'$, somit haben A und a' und daher auch a und A' entgegengesetzte Zeichen, woraus folgt: $\sqrt{D - \frac{aA'}{\delta^2}} > \sqrt{D} > b$. Hieraus geht hervor, dass in [4] notwendig das untere Zeichen genommen werden muss, weil bei dem oberen Zeichen $\frac{\beta}{\delta}$ offenbar dasselbe Zeichen erhalten würde, wie a. Es wird daher $\frac{\beta}{\delta} > \frac{-\sqrt{D}-b}{a} > 1$ (weil nach der Definition der reducierten Form $a < \sqrt{D} + b$ ist). Dies ist aber absurd, da $\beta = \pm 1$ und δ nicht gleich Null ist.

2. Es sei $\beta = 0$. Dann ergiebt sich aus der Gleichung $\alpha\delta - \beta\gamma = \pm 1$: $\alpha = \pm 1$, $\delta = \pm 1$. Hiernach folgt aus [2]: $-A' = -a'$; somit werden a' und a und A dasselbe Zeichen haben, woraus folgt: $\sqrt{D + \frac{aA}{\alpha^2}} > \sqrt{D} > b$. Hieraus geht hervor, dass in der Gleichung [3] das untere Zeichen genommen werden muss, weil bei dem oberen $\frac{\alpha}{\gamma}$ dasselbe Zeichen erhalten würde wie a. Es wird daher $\frac{\alpha}{\gamma} > \frac{-\sqrt{D}-b}{a} > 1$, und dies ist absurd aus demselben Grunde wie vorher.

Nehmen wir an, für den zweiten Teil des Satzes, dass weder $\alpha = 0$ noch $\beta = 0$ sei, dass $\frac{\gamma}{\alpha}$, $\frac{\delta}{\beta}$ nicht das dem Vorzeichen von a' entgegengesetzte Vorzeichen haben und dass

1. $\gamma = 0$ sei, so ist der Gleichung $\alpha\delta - \beta\gamma = \pm 1$ zufolge $\alpha = \pm 1$, $\delta = \pm 1$, demnach aus [1]: $A = a$; mithin werden A' und a' dasselbe Zeichen haben, woraus folgt: $\sqrt{D + \frac{a'A'}{\beta^2}} > \sqrt{D} > b$. Daher muss in [6] das obere Vorzeichen genommen werden, weil bei dem unteren $\frac{\delta}{\beta}$ das entgegengesetzte Zeichen erhalten würde wie a'. Es wird also $\frac{\delta}{\beta} > \frac{\sqrt{D}+b}{a'} > 1$. Dies ist aber absurd, da $\delta = \pm 1$ und β nicht gleich Null ist.

2. Ist endlich $\delta = 0$, so ist der Gleichung $\alpha\delta - \beta\gamma = \pm 1$ zufolge $\beta = \pm 1$, $\gamma = \pm 1$ und daher nach [2]: $-A' = a$. Hieraus folgt: $\sqrt{D - \frac{a'A}{\alpha^2}} > \sqrt{D} > b$, weshalb in [5] das obere Zeichen zu nehmen ist. Demnach wird $\frac{\gamma}{\alpha} > \frac{\sqrt{D}+b}{a'} > 1$, und dies ist absurd. —

Mithin ist unser Satz in seiner ganzen Ausdehnung bewiesen.

Da der Unterschied zwischen $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$ gleich $\frac{1}{\gamma\delta}$ ist, so wird der Unterschied zwischen $\frac{\pm\sqrt{D}-b}{a}$ und $\frac{\alpha}{\gamma}$ oder $\frac{\beta}{\delta}$ kleiner als $\frac{1}{\gamma\delta}$ sein; zwischen $\frac{\pm\sqrt{D}-b}{a}$ aber und $\frac{\alpha}{\gamma}$ oder zwischen jener Grösse und $\frac{\beta}{\delta}$ kann kein Bruch liegen, dessen Nenner nicht grösser als γ oder δ wäre (vorstehender Hülfssatz). — Ebenso wird der Unterschied zwischen der Grösse $\frac{\pm\sqrt{D}+b}{a}$ und dem Bruche $\frac{\gamma}{\alpha}$ oder dem folgenden $\frac{\delta}{\beta}$ kleiner als $\frac{1}{\alpha\beta}$ sein, und zwischen jener Grösse und einem von diesen Brüchen kann kein Bruch liegen, dessen Nenner nicht grösser wäre als α und β.

192.

Aus der Anwendung des vorigen Satzes auf den Algorithmus des Artikels 188 folgt, dass die Grösse $\frac{\sqrt{D}-b}{a}$, welche wir mit L bezeichnen wollen, zwischen $\frac{\alpha'}{\gamma'}$ und $\frac{\beta'}{\delta'}$, zwischen $\frac{\alpha''}{\gamma''}$ und $\frac{\beta''}{\delta''}$, zwischen $\frac{\alpha'''}{\gamma'''}$ und $\frac{\beta'''}{\delta'''}$ u. s. w. (denn aus Artikel 189, 3 am Ende folgt leicht, dass keine dieser Grenzen das dem Vorzeichen von a entgegengesetzte Zeichen hat, weshalb der Wurzelgrösse $\sqrt{D}$ das positive Vorzeichen beigelegt werden muss) oder zwischen $\frac{\alpha'}{\gamma'}$ und $\frac{\alpha''}{\gamma''}$, zwischen $\frac{\alpha''}{\gamma''}$ und $\frac{\alpha'''}{\gamma'''}$, u. s. w. liegt. Daher werden sämtliche

Brüche $\frac{\alpha'}{\gamma'}$, $\frac{\alpha'''}{\gamma'''}$, $\frac{\alpha'''''}{\gamma'''''}$, ... auf der einen Seite von L und alle Brüche $\frac{\alpha''}{\gamma''}$, $\frac{\alpha''''}{\gamma''''}$, $\frac{\alpha''''''}{\gamma''''''}$, ... auf der andern Seite liegen. Da aber $\gamma' < \gamma'''$ ist, so liegt $\frac{\alpha'}{\gamma'}$ ausserhalb des Intervalls $\frac{\alpha'''}{\gamma'''}$ und L und aus analogem Grunde $\frac{\alpha''}{\gamma''}$ ausserhalb des Intervalls L und $\frac{\alpha''''}{\gamma''''}$, $\frac{\alpha'''}{\gamma'''}$ ausserhalb des Intervalls L und $\frac{\alpha'''''}{\gamma'''''}$, u. s. w. Hieraus ist klar, dass diese Grössen in folgender Reihenfolge liegen:

$$\frac{\alpha'}{\gamma'},\ \frac{\alpha'''}{\gamma'''},\ \frac{\alpha'''''}{\gamma'''''},\ \ldots,\ L,\ \ldots,\ \frac{\alpha''''''}{\gamma''''''},\ \frac{\alpha''''}{\gamma''''},\ \frac{\alpha''}{\gamma''}.$$

Die Differenz zwischen $\frac{\alpha'}{\gamma'}$ und L aber ist kleiner als die Differenz zwischen $\frac{\alpha'}{\gamma'}$ und $\frac{\alpha''}{\gamma''}$ d. h. kleiner als $\frac{1}{\gamma'\gamma''}$, und aus ähnlichem Grunde ist die Differenz zwischen $\frac{\alpha''}{\gamma''}$ und L kleiner als $\frac{1}{\gamma''\gamma'''}$ u. s. w. Daher nähern sich die Brüche $\frac{\alpha'}{\gamma'}$, $\frac{\alpha''}{\gamma''}$, $\frac{\alpha'''}{\gamma'''}$, ... immer mehr der Grenze L, und da γ', γ'', γ''', ... fortwährend bis ins Unendliche wachsen, so kann die Differenz der Brüche und der Grenze kleiner gemacht werden als eine beliebige gegebene Grösse.

Nach Art. 189 hat keine der Grössen $\frac{\gamma}{\alpha}$, $\frac{'\gamma}{'\alpha}$, $\frac{''\gamma}{''\alpha}$, ... dasselbe Zeichen wie a; hieraus folgt durch eine der vorigen durchaus analoge Schlussreihe, dass jene Grössen und die Grösse $\frac{-\sqrt{D}+b}{a'}$, welche wir mit L' bezeichnen wollen, in der folgenden Reihenfolge liegen:

$$\frac{\gamma}{\alpha},\ \frac{''\gamma}{''\alpha},\ \frac{''''\gamma}{''''\alpha},\ \ldots,\ L',\ \ldots,\ \frac{'''''\gamma}{'''''\alpha},\ \frac{'''\gamma}{'''\alpha},\ \frac{'\gamma}{'\alpha}.$$

Die Differenz aber zwischen $\frac{\gamma}{\alpha}$ und L' ist kleiner als $\frac{1}{'\alpha\alpha}$, die Differenz zwischen $\frac{'\gamma}{'\alpha}$ und L' kleiner als $\frac{1}{''\alpha'\alpha}$, u. s. w. Daher nähern sich die Brüche $\frac{\gamma}{\alpha}$, $\frac{'\gamma}{'\alpha}$, ... immer mehr der Grenze L' und die Differenz kann kleiner gemacht werden als eine beliebige gegebene Grösse.

In dem Beispiele des Artikels 188 ist $L = \frac{\sqrt{79}-8}{3} = 0{,}2960648$ und die Näherungsbrüche sind: $\frac{0}{1}$, $\frac{1}{3}$, $\frac{2}{7}$, $\frac{3}{10}$, $\frac{5}{17}$, $\frac{8}{27}$, $\frac{45}{152}$, $\frac{143}{483}$, ... Es ist

aber $\frac{143}{483} = 0{,}2960662$. — Ebendaselbst ist $L' = \frac{-\sqrt{79}+8}{5} = -0{,}1776388$ und die Näherungsbrüche sind: $\frac{0}{1}, -\frac{1}{5}, -\frac{1}{6}, -\frac{2}{11}, -\frac{3}{17}, -\frac{8}{45}, -\frac{27}{152}, -\frac{143}{805}, \ldots$ Es ist aber $\frac{143}{805} = 0{,}1776397$.

193.

Satz. Wenn die reducierten Formen f, F eigentlich äquivalent sind, so ist die eine in der Periode der andern enthalten.

Es sei $f = (a, b, -a')$, $F = (A, B, -A')$, die Determinante dieser Formen gleich D und es gehe jene in diese über durch die eigentliche Substitution $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$. Dann behaupte ich: Wenn man die Periode der Form f sucht und die nach beiden Seiten unendliche Reihe der reducierten Formen und Transformationen der Form f in diese ermittelt, wie dies in Artikel 188 geschehen ist, so ist entweder $+\mathfrak{A}$ gleich irgend einem Gliede der Reihe $\ldots\, ''\alpha, {}'\alpha, \alpha, \alpha', \alpha'', \ldots$ und wenn man dieses gleich $\alpha^{(m)}$ setzt, so ist $+\mathfrak{B} = \beta^{(m)}$, $+\mathfrak{C} = \gamma^{(m)}$, $+\mathfrak{D} = \delta^{(m)}$, oder es ist $-\mathfrak{A}$ gleich einem Gliede $\alpha^{(m)}$ und $-\mathfrak{B}, -\mathfrak{C}, -\mathfrak{D}$ respective gleich $\beta^{(m)}, \gamma^{(m)}, \delta^{(m)}$ (wo m auch einen negativen Index bezeichnen kann). In beiden Fällen ist offenbar F identisch mit $f^{(m)}$.

Beweis. I. Man hat die vier Gleichungen:

[1] $$a\mathfrak{A}^2 + 2b\mathfrak{A}\mathfrak{C} - a'\mathfrak{C}^2 = A$$
[2] $$a\mathfrak{A}\mathfrak{B} + b(\mathfrak{A}\mathfrak{D} + \mathfrak{B}\mathfrak{C}) - a'\mathfrak{C}D = B$$
[3] $$a\mathfrak{B}^2 + 2b\mathfrak{B}\mathfrak{D} - a'D^2 = -A'$$
[4] $$\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C} = 1.$$

Wir betrachten aber zuerst den Fall, wo irgend eine der Zahlen $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$ gleich Null ist.

1. Wenn $\mathfrak{A} = 0$ ist, so folgt aus [4] $\mathfrak{B}\mathfrak{C} = -1$ und daher $\mathfrak{B} = \pm 1$, $\mathfrak{C} = \mp 1$. Hiernach ergiebt sich aus [1]: $-a' = A$, aus [2]: $-b \pm a'\mathfrak{D} = B$ oder $B \equiv -b$ (mod. a' oder A), woraus folgt, dass die Form $(A, B, -A')$ der Form $(a, b, -a')$ nach rechts hin benachbart ist. Da aber jene reduciert ist, so ist sie notwendig mit f' identisch. Demnach ist $B = b'$ und daher nach [2]: $b + b' = -a'\mathfrak{C}\mathfrak{D} = \pm a'\mathfrak{D}$; hieraus folgt, da $\frac{b+b'}{-a'} = h'$ ist, $\mathfrak{D} = \mp h'$. Hieraus schliesst man, dass $\mp\mathfrak{A}, \mp\mathfrak{B}, \mp\mathfrak{C}, \mp\mathfrak{D}$ respective gleich $0, -1, +1, h'$ oder gleich $\alpha', \beta', \gamma', \delta'$ sind.

2. Ist $\mathfrak{B} = 0$, so folgt aus [4]: $\mathfrak{A} = \pm 1$, $\mathfrak{D} = \pm 1$; aus [3]: $a' = A'$, aus [2]: $b \mp a'\mathfrak{C} = B$ oder $b \equiv B$ (mod. a'). Da aber sowohl f als F reducierte Formen sind, so wird sowohl b als B zwischen $\sqrt{D}$ und $\sqrt{D} \mp a'$ liegen (je nachdem a' positiv oder negativ ist, Artikel 184, 5). Daher ist notwendig $b = B$ und $\mathfrak{C} = 0$. Demnach sind die Formen f

und F identisch und $\pm\mathfrak{A}$, $\pm\mathfrak{B}$, $\pm\mathfrak{C}$, $\pm\mathfrak{D}$ respective gleich 1, 0, 0, 1 oder gleich α, β, γ, δ respective.

3. Ist $\mathfrak{C}=0$, so folgt aus [4]: $\mathfrak{A}=\pm 1$, $\mathfrak{D}=\pm 1$, aus [1]: $a=A$, aus [2]: $\pm a\mathfrak{B}+b=B$ oder $b\equiv B \pmod{a}$. Weil aber sowohl b als B zwischen $\sqrt{D}$ und $\sqrt{D}\mp a$ liegen, so wird notwendig $B=b$ und $\mathfrak{B}=0$ sein. Daher ist dieser Fall vom vorhergehenden nicht verschieden.

4. Ist $\mathfrak{D}=0$, so folgt aus [4]: $\mathfrak{B}=\pm 1$, $\mathfrak{C}=\mp 1$, aus [3]: $a=-A'$, aus [2]: $\pm a\mathfrak{A}-b=B$ oder $B\equiv -b \pmod{a}$. Hiernach ist F der Form f nach links hin benachbart und somit mit der Form $'f$ identisch. Wegen $\frac{'b+b}{a}=h$ und $B='b$ wird daher $\pm\mathfrak{A}=h$. Hieraus folgt, dass $\pm\mathfrak{A}$, $\pm\mathfrak{B}$, $\pm\mathfrak{C}$, $\pm\mathfrak{D}$ respective gleich h, 1, -1, 0 oder gleich $'\alpha$, $'\beta$, $'\gamma$, $'\delta$ sind.

Es bleibt daher nur der Fall übrig, wo keine der Zahlen $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ gleich Null ist. Hier werden dem Hülfssatze des Artikels 190 zufolge die Grössen $\frac{\mathfrak{A}}{\mathfrak{C}}$, $\frac{\mathfrak{B}}{\mathfrak{D}}$, $\frac{\mathfrak{C}}{\mathfrak{A}}$, $\frac{\mathfrak{D}}{\mathfrak{B}}$ dasselbe Zeichen haben, und es werden sich daher zwei Fälle ergeben, da dieses Zeichen entweder mit dem Zeichen von a, a' übereinstimmen oder ihm entgegengesetzt sein kann.

II. Wenn $\frac{\mathfrak{A}}{\mathfrak{C}}$, $\frac{\mathfrak{B}}{\mathfrak{D}}$ dasselbe Zeichen haben wie a, so wird die Grösse $\frac{\sqrt{D}-b}{a}$ (die wir mit L bezeichnen wollen) zwischen diesen Brüchen liegen (Artikel 191). Wir werden nun zeigen, dass $\frac{\mathfrak{A}}{\mathfrak{C}}$ irgend einem der Brüche $\frac{\alpha''}{\gamma''}$, $\frac{\alpha'''}{\gamma'''}$, $\frac{\alpha''''}{\gamma''''}$, $\cdots$ und $\frac{\mathfrak{B}}{\mathfrak{D}}$ dem nächstfolgenden gleich ist, oder dass, wenn $\frac{\mathfrak{A}}{\mathfrak{C}}=\frac{\alpha^{(m)}}{\gamma^{(m)}}$ ist, $\frac{\mathfrak{B}}{\mathfrak{D}}=\frac{\alpha^{(m+1)}}{\gamma^{(m+1)}}$ sein wird. Im vorigen Artikel zeigten wir, dass die Grössen $\frac{\alpha'}{\gamma'}$, $\frac{\alpha''}{\gamma''}$, $\frac{\alpha'''}{\gamma'''}$, $\cdots$ (die wir kurz mit (1), (2), (3), ... bezeichnen wollen) sowie L die folgende Reihenfolge (I) einhalten: (1), (3), (5), ..., L, ..., (6), (4), (2); die erste von diesen Grössen ist gleich Null (wegen $\alpha'=0$), die anderen haben dasselbe Zeichen wie L oder a. Da aber nach Voraussetzung $\frac{\mathfrak{A}}{\mathfrak{C}}$, $\frac{\mathfrak{B}}{\mathfrak{D}}$ (für die wir $\mathfrak{M}$, $\mathfrak{N}$ schreiben werden) dasselbe Zeichen haben, so werden offenbar diese Grössen rechts von (1) (oder, wenn man lieber will, auf derselben Seite wie L) liegen und zwar, da L zwischen ihnen liegt, die eine rechts von L, die andere links von L. Man kann aber leicht zeigen, dass $\mathfrak{M}$ nicht rechts von (2) liegen kann, denn sonst würde $\mathfrak{N}$ zwischen (1) und L liegen, woraus folgen würde, erstens dass (2) zwischen $\mathfrak{M}$ und $\mathfrak{N}$ liegt und daher der Nenner des Bruches (2) grösser ist als der Nenner des Bruches $\mathfrak{N}$ (Artikel 190), zweitens das $\mathfrak{N}$ zwischen (1) und (2) liegt und daher der Nenner des Bruches $\mathfrak{N}$ grösser ist als der Nenner des Bruches (2), was absurd ist.

Wir wollen annehmen, dass $\mathfrak{M}$ keinem der Brüche (2), (3), (4), ... gleich sei, und zusehen, was daraus folgt. Dann wird offenbar, wenn der Bruch $\mathfrak{M}$ links von L liegt, derselbe notwendig zwischen (1) und (3) oder zwischen (3) und (5) oder zwischen (5) und (7) u. s. w. liegen müssen (da L irrational und somit sicher von $\mathfrak{M}$ verschieden ist und die Brüche (1), (3), (5), ... bis auf eine beliebig gegebene von L verschiedene Grösse an L heranrücken können). Wenn aber $\mathfrak{M}$ rechts von L liegt, so wird es notwendig entweder zwischen (2) und (4) oder zwischen (4) und (6) oder zwischen (6) und (8) u. s. w. liegen. Nehmen wir daher an, dass $\mathfrak{M}$ zwischen (m) und $(m+2)$ liege, so werden offenbar die Grössen $\mathfrak{M}$, (m), $(m+1)$, $(m+2)$, L in der folgenden Reihenfolge liegen:

(II)*) $\qquad (m),\ \mathfrak{M},\ (m+2),\ L,\ (m+1).$

Dann ist notwendig $\mathfrak{N}=(m+1)$. Denn es liegt $\mathfrak{N}$ rechts von L; wenn es aber auch rechts von $(m+1)$ läge, so würde $(m+1)$ zwischen $\mathfrak{M}$ und $\mathfrak{N}$ liegen, also $\gamma^{(m+1)}>\mathfrak{C}$ sein, $\mathfrak{M}$ aber zwischen (m) und $(m+1)$ liegen, also $C>\gamma^{(m+1)}$ sein (Artikel 190), was absurd ist. Wenn aber $\mathfrak{N}$ links von $(m+1)$ läge oder zwischen $(m+2)$ und $(m+1)$, so würde $\mathfrak{D}>\gamma^{(m+2)}$ sein, und da $(m+2)$ zwischen $\mathfrak{M}$ und $\mathfrak{N}$ liegt, würde $\gamma^{(m+2)}>\mathfrak{D}$ sein, was absurd ist. Es ist daher $\mathfrak{N}=(m+1)$ oder $\frac{\mathfrak{B}}{\mathfrak{D}}=\frac{\alpha^{(m+1)}}{\gamma^{(m+1)}}=\frac{\beta^{(m)}}{\delta^{(m)}}$.

Da $\mathfrak{A}\mathfrak{D}-\mathfrak{B}\mathfrak{C}=1$ ist, so ist $\mathfrak{B}$ prim zu $\mathfrak{D}$ und aus ähnlichem Grunde $\beta^{(m)}$ prim zu $\delta^{(m)}$. Hieraus erkennt man leicht, dass die Gleichung $\frac{\mathfrak{B}}{\mathfrak{D}}=\frac{\beta^{(m)}}{\delta^{(m)}}$ nur bestehen kann, wenn entweder $\mathfrak{B}=\beta^{(m)}$, $\mathfrak{D}=\delta^{(m)}$ oder $\mathfrak{B}=-\beta^{(m)}$, $\mathfrak{D}=-\delta^{(m)}$ ist. Da nun die Form f durch die eigentliche Substitution $\alpha^{(m)}$, $\beta^{(m)}$, $\gamma^{(m)}$, $\delta^{(m)}$ in die Form $f^{(m)}$, welche $(\pm a^{(m)}, b^{(m)}, \mp a^{(m+1)})$ lautet, übergeht, so hat man die Gleichungen:

[5] $$a\alpha^{(m)2}+2b\alpha^{(m)}\gamma^{(m)}-a'\gamma^{(m)2}=\pm a^{(m)}$$

[6] $$a\alpha^{(m)}\beta^{(m)}+b(\alpha^{(m)}\delta^{(m)}+\beta^{(m)}\gamma^{(m)})-a'\gamma^{(m)}\delta^{(m)}=b^{(m)}$$

[7] $$a\beta^{(m)2}+2b\beta^{(m)}\delta^{(m)}-a'\delta^{(m)2}=\mp a^{(m+1)}$$

[8] $$\alpha^{(m)}\delta^{(m)}-\beta^{(m)}\gamma^{(m)}=1.$$

Hiernach wird (aus der Gleichung [7] und [3]): $\mp a^{(m+1)}=-A'$. Multipliciert man ferner die Gleichung [2] mit $\alpha^{(m)}\delta^{(m)}-\beta^{(m)}\gamma^{(m)}$, die Gleichung [6] mit $\mathfrak{A}\mathfrak{D}-\mathfrak{B}\mathfrak{C}$ und subtrahiert man, so bestätigt man leicht durch Entwicklung die Gleichung:

[9] $$\begin{aligned}B-b^{(m)}=(\mathfrak{C}\alpha^{(m)}-\mathfrak{A}\gamma^{(m)})\,[a\mathfrak{B}\beta^{(m)}+b(\mathfrak{D}\beta^{(m)}+\mathfrak{B}\delta^{(m)})-a'\mathfrak{D}\delta^{(m)}]\\+(\mathfrak{B}\delta^{(m)}-\mathfrak{D}\beta^{(m)})\,[a\mathfrak{A}\alpha^{(m)}+b(\mathfrak{C}\alpha^{(m)}+\mathfrak{A}\gamma^{(m)})-a'\mathfrak{C}\gamma^{(m)}],\end{aligned}$$

*) Es ist hier gleichgültig, mag die Reihenfolge in (II) dieselbe oder die entgegengesetzte wie in (I) sein, d. h. mag (m) auch in (I) links oder rechts von L liegen.

oder, da entweder $\beta^{(m)} = \mathfrak{B}$, $\delta^{(m)} = \mathfrak{D}$ oder $\beta^{(m)} = -\mathfrak{B}$, $\delta^{(m)} = -\mathfrak{D}$ ist:

$$B - b^{(m)} = \pm(\mathfrak{C}\alpha^{(m)} - \mathfrak{A}\gamma^{(m)})(a\mathfrak{B}^2 + 2b\mathfrak{B}\mathfrak{D} - a'\mathfrak{D}^2) = \mp(\mathfrak{C}\alpha^{(m)} - \mathfrak{A}\gamma^{(m)})A'.$$

Hiernach ist $B \equiv b^{(m)}$ (mod. A'). Da aber sowohl B als auch $b^{(m)}$ zwischen $\sqrt{D}$ und $\sqrt{D} \mp A'$ liegen, so ist notwendig $B = b^{(m)}$ und daher $\mathfrak{C}\alpha^{(m)} - \mathfrak{A}\gamma^{(m)} = 0$, oder $\frac{\mathfrak{A}}{\mathfrak{C}} = \frac{\alpha^{(m)}}{\gamma^{(m)}}$, d. h. $\mathfrak{M} = (m)$.

Auf diese Weise haben wir also aus der Annahme, dass $\mathfrak{M}$ keiner der Grössen (2), (3), (4), ... gleich sei, abgeleitet, dass es in der That irgend einer von ihnen gleich ist. Wenn wir nun aber von Anfang an annehmen, dass $\mathfrak{M} = (m)$ sei, so wird offenbar entweder $\mathfrak{A} = \alpha^{(m)}$ und $\mathfrak{C} = \gamma^{(m)}$ oder $-\mathfrak{A} = \alpha^{(m)}$, $-\mathfrak{C} = \gamma^{(m)}$. In beiden Fällen folgt aus [1] und [5]: $A = \pm a^{(m)}$ und aus [9]: $B - b^{(m)} = \pm(\mathfrak{B}\delta^{(m)} - \mathfrak{D}\beta^{(m)})A$ oder $B \equiv b^{(m)}$ (mod. A). Hieraus ergiebt sich in ähnlicher Weise wie oben $B = b^{(m)}$ und hieraus $\mathfrak{B}\delta^{(m)} = \mathfrak{D}\beta^{(m)}$; da nun $\mathfrak{B}$ zu $\mathfrak{D}$ prim ist und $\beta^{(m)}$ zu $\delta^{(m)}$, so ist demnach entweder $\mathfrak{B} = \beta^{(m)}$, $\mathfrak{D} = \delta^{(m)}$ oder $\mathfrak{B} = -\beta^{(m)}$, $\mathfrak{D} = -\delta^{(m)}$ und somit folgt aus [7]: $-A' = \mp a^{(m+1)}$. Demnach sind die Formen F und $f^{(m)}$ identisch. Mit Hülfe der Gleichung $\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C} = \alpha^{(m)}\delta^{(m)} - \beta^{(m)}\gamma^{(m)}$ beweist man aber ohne Mühe, dass $+\mathfrak{B} = \beta^{(m)}$, $+\mathfrak{D} = \delta^{(m)}$, falls $+\mathfrak{A} = \alpha^{(m)}$, $+\mathfrak{C} = \gamma^{(m)}$ ist, dagegen $-\mathfrak{B} = \beta^{(m)}$, $-\mathfrak{D} = \delta^{(m)}$ gesetzt werden muss, falls $-\mathfrak{A} = \alpha^{(m)}$, $-\mathfrak{C} = \gamma^{(m)}$ ist. Dies sollte bewiesen werden.

III. Wenn das Zeichen der Grössen $\frac{\mathfrak{A}}{\mathfrak{C}}$, $\frac{\mathfrak{B}}{\mathfrak{D}}$ dem Zeichen von a entgegengesetzt ist, ist der Beweis dem vorstehenden so ähnlich, dass es genügt, nur die Hauptpunkte anzudeuten. Es liegt $\frac{-\sqrt{D} + b}{a'}$ zwischen $\frac{\mathfrak{C}}{\mathfrak{A}}$ und $\frac{\mathfrak{D}}{\mathfrak{B}}$. Der Bruch $\frac{\mathfrak{D}}{\mathfrak{B}}$ ist irgend einem der Brüche

$$\text{(I)} \qquad \frac{'\delta}{'\beta}, \; \frac{''\delta}{''\beta}, \; \frac{'''\delta}{'''\beta}, \; \cdots$$

gleich, und wird derselbe gleich $\frac{^{(m)}\delta}{^{(m)}\beta}$ gesetzt, so ist

$$\text{(II)} \qquad \frac{\mathfrak{C}}{\mathfrak{A}} = \frac{^{(m)}\gamma}{^{(m)}\alpha}.$$

(I) aber wird folgendermassen bewiesen. Wenn angenommen wird, dass $\frac{\mathfrak{D}}{\mathfrak{B}}$ keinem jener Brüche gleich ist, so muss es zwischen zwei solchen $\frac{^{(m)}\delta}{^{(m)}\beta}$ und $\frac{^{(m+2)}\delta}{^{(m+1)}\beta}$ liegen. Hieraus aber folgt auf dieselbe Weise wie oben, dass notwendig

$$\frac{\mathfrak{C}}{\mathfrak{A}} = \frac{{}^{(m+1)}\delta}{{}^{(m+1)}\beta} = \frac{{}^{(m)}\gamma}{{}^{(m)}\alpha}$$

und daher entweder $\mathfrak{A} = {}^{(m)}\alpha$, $\mathfrak{C} = {}^{(m)}\gamma$ oder $-\mathfrak{A} = {}^{(m)}\alpha$, $-\mathfrak{C} = {}^{(m)}\gamma$ ist. Da aber f durch die eigentliche Substitution ${}^{(m)}\alpha$, ${}^{(m)}\beta$, ${}^{(m)}\gamma$, ${}^{(m)}\delta$ in die Form

$${}^{(m)}f = (\pm\, {}^{(m)}a,\ {}^{(m)}b,\ \mp\, {}^{(m-1)}a)$$

übergeht, so ergeben sich drei Gleichungen, aus denen in Verbindung mit den Gleichungen [1], [2], [3], [4] und der folgenden ${}^{(m)}\alpha\, {}^{(m)}\delta - {}^{(m)}\beta\, {}^{(m)}\gamma = 1$ in derselben Weise wie oben hervorgeht, dass das erste Glied A der Form F dem ersten Gliede der Form ${}^{(m)}f$ gleich und das mittlere Glied jener dem mittleren Gliede dieser nach dem Modul A congruent ist. Hieraus folgt, da beide Formen reduciert sind und daher das mittlere Glied beider zwischen $\sqrt{D}$ und $\sqrt{D} \mp A$ liegt, dass diese mittleren Glieder gleich sind, und hieraus leitet man her, dass $\frac{{}^{(m)}\delta}{{}^{(m)}\beta} = \frac{\mathfrak{D}}{\mathfrak{B}}$ ist. Demnach ist hier die Richtigkeit der Behauptung (I) aus der Annahme, dass sie falsch sei, abgeleitet.

Nimmt man aber $\frac{{}^{(m)}\delta}{{}^{(m)}\beta} = \frac{\mathfrak{D}}{\mathfrak{B}}$ an, so wird auf ganz analoge Weise und durch dieselben Gleichungen bewiesen, dass auch $\frac{{}^{(m)}\gamma}{{}^{(m)}\alpha} = \frac{\mathfrak{C}}{\mathfrak{A}}$ ist, was (II) war. Hieraus aber folgt mit Hülfe der Gleichungen $\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C} = 1$, ${}^{(m)}\alpha\, {}^{(m)}\delta - {}^{(m)}\beta\, {}^{(m)}\gamma = 1$, dass

entweder $\mathfrak{A} = {}^{(m)}\alpha$, $\mathfrak{B} = {}^{(m)}\beta$, $\mathfrak{C} = {}^{(m)}\gamma$, $\mathfrak{D} = {}^{(m)}\delta$
oder $-\mathfrak{A} = {}^{(m)}\alpha$, $-\mathfrak{B} = {}^{(m)}\beta$, $-\mathfrak{C} = {}^{(m)}\gamma$, $-\mathfrak{D} = {}^{(m)}\delta$

ist, und dass die Formen F und ${}^{(m)}f$ identisch sind, und dies sollte bewiesen werden.

194.

Da die Formen, welche wir oben (Artikel 187, 6) associiierte Formen genannt haben, stets uneigentlich äquivalent sind (Artikel 159), so ist klar, dass, wenn die reducierten Formen F, f uneigentlich äquivalent sind und die zur Form F associiierte Form G ist, die Formen f, G eigentlich äquivalent sind und daher die Form G in der Periode der Form f enthalten ist. Wenn daher die Formen F und f sowohl eigentlich als auch uneigentlich äquivalent sind, so wird sich offenbar sowohl F als auch G in der Periode der Form f vorfinden müssen. Demnach wird diese Periode sich selbst associiert sein und zwei ambige Formen enthalten (Artikel 187, 7). Hierdurch erhalten wir eine schöne Bestätigung des Satzes im Artikel 165, demzufolge wir bereits hätten gewiss sein können, dass es irgend eine ambige Form giebt, die den Formen F, f äquivalent ist.

195.

Aufgabe. Wenn irgend zwei Formen Φ und φ mit derselben Determinante gegeben sind, so soll man entscheiden, ob sie äquivalent sind oder nicht.

Auflösung. Man suche zwei reducierte Formen F und f, welche den gegebenen Formen Φ und φ respective äquivalent sind (Artikel 183). Je nachdem diese entweder nur eigentlich oder nur uneigentlich oder auf beide Arten oder auf keinerlei Weise äquivalent sind, werden auch die gegebenen Formen entweder nur eigentlich oder nur uneigentlich oder auf beide Arten oder gar nicht äquivalent sein. Man entwickle die Periode der einen von diesen beiden reducierten Formen, z. B. die Periode der Form f. Wenn die Form F in dieser Periode vorkommt und nicht zugleich auch die zu F associierte Form, so wird offenbar der erste Fall stattfinden. Kommt dagegen diese associierte Form vor, aber nicht F selbst, so findet der zweite, wenn beide Formen vorkommen, der dritte, wenn keine der beiden Formen vorkommt, der vierte Fall statt.

Beispiel. Gegeben seien die Formen (129, 92, 65), (42, 59, 81) mit der Determinante 79. Als diesen äquivalente reducierte Formen findet man (10, 7, — 3), (5, 8, — 3). Die Periode der ersteren Form ist folgende: (10, 7, — 3), (— 3, 8, 5), (5, 7, — 6), (— 6, 5, 9), (9, 4, — 7), (— 7, 3, 10). Da sich in dieser die Form (5, 8, — 3) selbst nicht findet, wohl aber die ihr associierte Form (— 3, 8, 5), so folgt, dass die gegebenen Formen nur uneigentlich äquivalent sind.

Wenn alle reducierten Formen mit derselben Determinante in derselben Weise wie oben (Artikel 187, 5) in Perioden $P, Q, R, \ldots$ verteilt werden und aus jeder Periode irgend eine Form nach Belieben ausgewählt wird, aus P F, aus Q G, aus R H u. s. w., so können unter diesen Formen $F, G, H, \ldots$ keine zwei vorkommen, welche eigentlich äquivalent sind. Jede andere Form mit derselben Determinante aber wird irgend einer von diesen und zwar nur einer eigentlich äquivalent sein. Hieraus geht hervor, dass sämtliche Formen mit dieser Determinante in ebenso viele **Klassen** verteilt werden können, als man Perioden hat, indem man nämlich diejenigen, welche der Form F eigentlich äquivalent sind, in die erste Klasse, diejenigen, welche der Form G eigentlich äquivalent sind, in die zweite Klasse, u. s. w. setzt. Auf diese Weise werden alle in derselben Klasse enthaltenen Formen eigentlich äquivalent sein; Formen aus verschiedenen Klassen aber werden nicht eigentlich äquivalent sein können. Doch halten wir uns hier bei diesem Gegenstande, der unten näher auseinandergesetzt werden soll, nicht auf.

196.

Aufgabe. Wenn zwei eigentlich äquivalente Formen Φ und φ gegeben sind, so soll man eine eigentliche Transformation der einen in die andere finden.

Auflösung. Nach der Methode des Artikels 183 kann man zwei Reihen von Formen

$$\Phi,\ \Phi',\ \Phi'',\ \ldots,\ \Phi^{(n)} \text{ und } \varphi,\ \varphi',\ \varphi'',\ \ldots,\ \varphi^{(\nu)}$$

von der Beschaffenheit finden, dass jede folgende Form der vorhergehenden eigentlich äquivalent ist und die letzten $\Phi^{(n)}$ und $\varphi^{(\nu)}$ reducierte Formen sind; und da wir vorausgesetzt haben, dass Φ und φ eigentlich äquivalent sind, so wird notwendig $\Phi^{(n)}$ in der Periode der Form $\varphi^{(\nu)}$ vorkommen. Es sei $\varphi^{(\nu)} = f$ und deren Periode bis zur Form $\Phi^{(n)}$ die folgende:

$$f,\ f'\ f'',\ \ldots,\ f^{(m-1)},\ \Phi^{(n)},$$

so dass in dieser Periode der Index der Form $\Phi^{(n)}$ gleich m ist, und man bezeichne diejenigen Formen, welche den associierten Formen von $\Phi, \Phi', \Phi'', \ldots, \Phi^{(n)}$ entgegengesetzt sind, respective mit

$$\Psi,\ \Psi',\ \Psi'',\ \ldots,\ \Psi^{(n)}.\text{*)}$$

Dann wird in der Reihe

$$\varphi,\ \varphi',\ \varphi'',\ \ldots,\ f,\ f',\ f'',\ \ldots,\ f^{(m-1)},\ \Psi^{(n-1)},\ \Psi^{(n-2)},\ \ldots,\ \Psi,\ \Phi$$

jede Form der vorhergehenden nach rechts hin benachbart sein, und somit lässt sich nach Artikel 177 eine eigentliche Transformation der ersten Form φ in die letzte Φ finden. Jenes ist bei den übrigen Formen der Reihe ohne Weiteres ersichtlich. Für die Formen $f^{(m-1)}, \Psi^{(n-1)}$ ist der Beweis folgendermassen. Es sei

$$f^{(m-1)} = (g,\ h,\ i),\ f^{(m)} \text{ oder } \Phi^{(n)} = (g',\ h',\ i'),\quad \Phi^{(n-1)} = (g'',\ h'',\ i'').$$

Die Form (g', h', i') wird sowohl der Form (g, h, i) als auch der Form (g'', h'', i'') nach rechts hin benachbart sein, hiernach ist $i = g' = i''$ und $-h \equiv h' \equiv -h''$ (mod. i oder g' oder i''). Hieraus geht hervor, dass die Form $(i'', -h'', g'')$ d. i. die Form $\Psi^{(n-1)}$ der Form (g, h, i) d. i. der Form $f^{(m-1)}$ nach rechts hin benachbart ist.

Wenn die Formen Φ, φ uneigentlich äquivalent sind, so wird die Form φ derjenigen Form, welcher Φ entgegengesetzt ist, eigentlich äquivalent sein. Man kann daher eine eigentliche Transformation der Form φ in diejenige Form, welcher Φ entgegengesetzt ist, finden. Nimmt man an, dass dies durch die Substitution $\alpha, \beta, \gamma, \delta$ geschieht, so erkennt man leicht, dass φ in Φ selbst durch die Substitution $\alpha, -\beta, \gamma, -\delta$ uneigentlich transformiert wird.

Hieraus ist auch ersichtlich, dass, wenn die Formen Φ und φ sowohl eigentlich als auch uneigentlich äquivalent sind, zwei Transformationen, eine eigentliche und eine uneigentliche, gefunden werden können.

*) So dass also Ψ aus Φ entsteht, wenn man das erste und letzte Glied vertauscht und dem mittleren Gliede das entgegengesetzte Zeichen giebt; ebenso bei den andern.

Beispiel. Man sucht eine uneigentliche Transformation der Form (129, 92, 65) in die Form (42, 59, 81), die, wie wir im vorigen Artikel fanden, jener uneigentlich äquivalent ist. Man hat also zunächst eine eigentliche Transformation der Form (129, 92, 65) in die Form (42, —59, 81) zu suchen. Zu dem Ende entwickle man die folgende Reihe von Formen: (129, 92, 65), (65, —27, 10), (10, 7, —3), (—3, 8, 5), (5, 22, 81), (81, 59, 42), (42, —59, 81). Hieraus leitet man die eigentliche Transformation —47, 56, 73, —87 her, durch welche (129, 92, 65) in (42, —59, 81) übergeht. Erstere Form wird daher durch die uneigentliche Transformation —47, —56, 73, 87 in die Form (42, 59, 81) übergehen.

197.

Wenn man eine Transformation irgend einer Form (a, b, c) oder φ in eine äquivalente Form Φ hat, so kann man aus dieser sämtliche gleichartige Transformationen der Form φ in Φ ableiten, wofern man nur sämtliche Lösungen der unbestimmten Gleichung $t^2 - Du^2 = m^2$, in welcher D die Determinante der Formen Φ, φ und m den grössten gemeinschaftlichen Teiler der Zahlen a, $2b$, c (Artikel 162) bezeichnet, angeben kann. Dieses Problem, welches wir für einen negativen Wert von D bereits oben gelöst haben, werden wir jetzt auch für einen **positiven** Wert von D in Angriff nehmen. Weil aber offenbar jeder der Gleichung genügende Wert von t derselben auch nach Veränderung seines Zeichens genügt, und dasselbe von den Werten von u gilt, so werden wir nur alle positiven Werte von t, u zu bestimmen brauchen, und es wird jede Lösung durch positive Werte die Stelle von vier Lösungen vertreten. Diese Aufgabe werden wir dadurch erledigen, dass wir zunächst die **kleinsten** Werte von t, u (ausser den von selbst sich darbietenden $t = m$, $u = 0$) zu finden und sodann aus diesen alle übrigen abzuleiten lehren.

198.

Aufgabe. Man soll die kleinsten der unbestimmten Gleichung $t^2 - Du^2 = m^2$ genügenden Werte von t, u finden, wenn irgend eine Form (M, N, P) gegeben ist, deren Determinante gleich D und bei welcher der grösste gemeinschaftliche Teiler der Zahlen M, $2N$, P gleich m ist.

Auflösung. Man nehme nach Belieben eine reducierte Form $(a, b, -a')$ oder f mit der Determinante D, bei welcher der grösste gemeinschaftliche Teiler der Zahlen a, $2b$, a' gleich m ist. Dass es eine solche giebt, ist schon daraus ersichtlich, dass man eine der Form (M, N, P) äquivalente reducierte Form finden kann, welche nach Artikel 161 diese Eigenschaft besitzt; zum vorliegenden Zwecke aber kann man jede reducierte Form, in welcher diese Bedingung stattfindet, anwenden. Man entwickle die Periode der Form f, die, wie wir annehmen wollen, aus n Formen bestehen möge.

Mit Beibehaltung aller Bezeichnungen, deren wir uns im Artikel 188 bedienten, ist $f^{(n)} = (+a^{(n)}, b^{(n)}, -a^{(n+1)})$, weil n gerade ist, und in diese Form wird f übergehen durch die eigentliche Substitution $\alpha^{(n)}, \beta^{(n)}, \gamma^{(n)}, \delta^{(n)}$. Da aber f und $f^{(n)}$ identisch sind, so wird f in $f^{(n)}$ auch durch die eigentliche Substitution 1, 0, 0, 1 übergehen. Aus diesen beiden gleichartigen Transformationen der Form f in $f^{(n)}$ lässt sich nach Artikel 162 die Lösung der Gleichung $t^2 - Du^2 = m^2$ in ganzen Zahlen ableiten, nämlich $t = \frac{1}{2}(\alpha^{(n)} + \delta^{(n)})\, m$ (Gleichung 18 im Artikel 162), $u = \frac{\gamma^{(n)} m}{a}$ (Gleichung 19)*). Werden diese Werte, positiv genommen, wenn sie es noch nicht sein sollten, mit T, U bezeichnet, so werden T, U die kleinsten Werte von t, u ausser $t = m,\ u = 0$ sein (von welchen sie notwendig verschieden sind, da offenbar $\gamma^{(n)}$ nicht gleich Null sein kann).

Denn nehmen wir an, dass es noch kleinere Werte von t, u gebe, etwa $\mathfrak{t}$ und $\mathfrak{u}$, welche positiv sind und von denen $\mathfrak{u}$ nicht gleich Null ist, so wird nach Artikel 162 die Form f durch die eigentliche Substitution $\frac{1}{m}(\mathfrak{t} - b\mathfrak{u}),\ \frac{1}{m}a'\mathfrak{u},\ \frac{1}{m}a\mathfrak{u},\ \frac{1}{m}(\mathfrak{t} + b\mathfrak{u})$ in eine mit ihr identische Form übergehen. Nun folgt aus Artikel 193 II, dass entweder $\frac{1}{m}(\mathfrak{t} - b\mathfrak{u})$ oder $-\frac{1}{m}(\mathfrak{t} - b\mathfrak{u})$ irgend einer der Zahlen $\alpha'', \alpha''', \alpha'''', \ldots$ gleich sein muss, etwa gleich $\alpha^{(\mu)}$ (weil nämlich $\mathfrak{t}^2 = D\mathfrak{u}^2 + m^2 = b^2\mathfrak{u}^2 + aa'\mathfrak{u}^2 + m^2$ ist, so wird $\mathfrak{t}^2 > b^2\mathfrak{u}^2$ und daher $\mathfrak{t} - b\mathfrak{u}$ positiv; mithin wird der Bruch $\frac{\mathfrak{t} - b\mathfrak{u}}{a\mathfrak{u}}$, welcher dem Bruche $\frac{\mathfrak{A}}{\mathfrak{C}}$ im Artikel 193 entspricht, dasselbe Zeichen haben wie a oder a'), und dass im ersteren Falle $\frac{1}{m}a'\mathfrak{u},\ \frac{1}{m}a\mathfrak{u},\ \frac{1}{m}(\mathfrak{t} + b\mathfrak{u})$, im letzteren aber dieselben Grössen mit entgegengesetztem Vorzeichen respective gleich $\beta^{(\mu)}, \gamma^{(\mu)}, \delta^{(\mu)}$ sind. Da aber $\mathfrak{u} < U$ d. h. $\mathfrak{u} < \frac{\gamma^{(n)} m}{a}$ und > 0 ist, so wird $\gamma^{(\mu)} < \gamma^{(n)}$ und > 0 sein; daher wird, da die Reihe $\gamma, \gamma', \gamma'', \ldots$ beständig wächst, notwendig μ zwischen 0 und n exclusive liegen. Die entsprechende Form $f^{(\mu)}$ aber wird identisch sein mit der Form f: Dies ist aber absurd, da alle Formen $f, f', f'', \ldots$ bis zu $f^{(n-1)}$ als verschieden vorausgesetzt sind. Hieraus folgt, dass T, U die kleinsten Werte von t, u (mit Ausnahme von m, 0) sind.

Beispiel. Ist $D = 79$, $m = 1$, so kann man die Form $(3, 8, -5)$ anwenden, für welche $n = 6$, und $\alpha^{(n)} = -8$, $\gamma^{(n)} = -27$, $\delta^{(n)} = -152$ ist

---

*) Was im Artikel 162 war:

	$\alpha, \beta, \gamma, \delta$;	$\alpha', \beta', \gamma', \delta'$;	A, B, C;	a, b, c;	e
ist hier:	1, 0, 0, 1;	$\alpha^{(n)}, \beta^{(n)}, \gamma^{(n)}, \delta^{(n)}$;	$a, b, -a'$;	$a, b, -a'$;	1.

(Artikel 188). Hieraus folgt $T = 80$, $U = 9$, welches die kleinsten der Gleichung $t^2 - 79u^2 = 1$ genügenden Werte der Zahlen t, u sind.

199.

Für die Praxis können noch bequemere Formeln aufgestellt werden. Es wird nämlich $2b\gamma^{(n)} = -a(\alpha^{(n)} - \delta^{(n)})$, was aus Artikel 162 leicht folgt, wenn man die Gleichung [19] mit $2b$, [20] mit a multipliciert und die dort gebrauchten Bezeichnungen mit den gegenwärtigen vertauscht. Hieraus wird $\alpha^{(n)} + \delta^{(n)} = 2\delta^{(n)} - \frac{2b}{a}\gamma^{(n)}$ und daher:

$$\pm T = m\left(\delta^{(n)} - \frac{b}{a}\gamma^{(n)}\right), \quad \pm U = \frac{\gamma^{(n)} m}{a}.$$

Durch eine ähnliche Methode erhält man die folgenden Werte:

$$\pm T = m\left(\alpha^{(n)} + \frac{b}{a'}\beta^{(n)}\right), \quad \pm U = \frac{\beta^{(n)} m}{a'}.$$

Sowohl jene wie diese Formeln werden sehr bequem, da $\gamma^{(n)} = \delta^{(n-1)}$, $\alpha^{(n)} = \beta^{(n-1)}$ ist, so dass man, wenn man sich dieser bedient, nur die Reihe $\beta', \beta'', \beta''', \ldots, \beta^{(n)}$, wenn man aber jene anwendet, nur die Reihe $\delta', \delta'', \delta''', \ldots$ zu berechnen braucht. Ausserdem folgt aus Artikel 189, 3 leicht, da n notwendig gerade ist, dass $\alpha^{(n)}$ und $\frac{b}{a'}\beta^{(n)}$ dasselbe Zeichen haben, ebenso $\delta^{(n)}$ und $\frac{b}{a}\gamma^{(n)}$, so dass man in der ersten Formel die absolute Differenz, in der letzten die absolute Summe nehmen muss und daher auf die Vorzeichen überhaupt keine Rücksicht zu nehmen braucht. Bei Wiederaufnahme der im Artikel 189, 4 angewendeten Bezeichnungen wird aus der ersten Formel:

$$T = m[k', k'', k''', \ldots, k^{(n)}] - \frac{mb}{a}[k', k'', k''', \ldots, k^{(n-1)}],$$

$$U = \frac{m}{a}[k', k'', k''', \ldots, k^{(n-1)}],$$

aus der zweiten:

$$T = m[k'', k''', \ldots, k^{(n-1)}] + \frac{mb}{a'}[k'', k''', \ldots, k^{(n)}],$$

$$U = \frac{m}{a'}[k'', k''', \ldots, k^{(n)}],$$

wo für den Wert von T auch $m\left[k'', k''', \ldots, k^{(n)}, \frac{b}{a'}\right]$ geschrieben werden kann.

Beispiel. Für $D=61$, $m=2$ kann man die Form $(2, 7, -6)$ anwenden, für welche man $n=6$, k', k'', k''', k'''', k''''', k'''''' respective gleich 2, 2, 7, 2, 2, 7 findet. Hieraus folgt:

$$T = 2[2, 2, 7, 2, 2, 7] - 7[2, 2, 7, 2, 2] = 2888 - 1365 = 1523$$

aus der ersten Formel; derselbe Wert ergiebt sich aus der zweiten:

$$T = 2[2, 7, 2, 2] + \tfrac{7}{3}[2, 7, 2, 2, 7]$$

$$U \text{ aber wird } = [2, 2, 7, 2, 2] = \tfrac{1}{3}[2, 7, 2, 2, 7] = 195.$$

Übrigens giebt es noch mancherlei Kunstgriffe, durch welche die Rechnungen zusammengezogen werden können; doch gestattet uns das Streben nach Kürze nicht, von ihnen weitläufiger zu reden.

200.

Um aus den kleinsten Werten von t, u sämtliche zu erhalten, stellen wir die Gleichung $T^2 - DU^2 = m^2$ so dar:

$$\left(\frac{T}{m} + \frac{U}{m}\sqrt{D}\right)\left(\frac{T}{m} - \frac{U}{m}\sqrt{D}\right) = 1,$$

woraus folgt, wenn e eine beliebige Zahl bezeichnet:

$$[1] \qquad \left(\frac{T}{m} + \frac{U}{m}\sqrt{D}\right)^e \cdot \left(\frac{T}{m} - \frac{U}{m}\sqrt{D}\right)^e = 1.$$

Wir wollen nun der Kürze wegen die Werte der Grössen

$$\frac{m}{2}\left(\frac{T}{m} + \frac{U}{m}\sqrt{D}\right)^e + \frac{m}{2}\left(\frac{T}{m} - \frac{U}{m}\sqrt{D}\right)^e,$$

$$\frac{m}{2\sqrt{D}}\left(\frac{T}{m} + \frac{U}{m}\sqrt{D}\right)^e - \frac{m}{2\sqrt{D}}\left(\frac{T}{m} - \frac{U}{m}\sqrt{D}\right)^e$$

allgemein mit $t^{(e)}$, $u^{(e)}$, d. h. die Werte jener für $e=0$ mit t^0, u^0 (welche gleich m, 0 sein werden), für $e=1$ mit t', u' (welche T, U sein werden), für $e=2$ mit t'', u'', für $e=3$ mit t''', u''' u. s. w. bezeichnen und werden beweisen, dass, wenn man für e alle nicht negativen ganzen Zahlen, d. h. 0 und alle positiven Zahlen von 1 bis ∞ nimmt, jene Ausdrücke sämtliche positiven Werte von t, u darstellen, nämlich I. dass alle Werte jener Ausdrücke in der That Werte von t, u sind, II. dass alle jene Werte ganze Zahlen sind; III. dass es keine positiven Werte von t, u giebt, welche nicht unter jenen Formeln enthalten sind.

I. Setzt man für $t^{(e)}$, $u^{(e)}$ ihre Werte, so bestätigt man ohne Mühe mit Hülfe der Gleichung [1], dass

$$(t^{(e)} + u^{(e)}\sqrt{D})(t^{(e)} - u^{(e)}\sqrt{D}) = m^2, \text{ d. h. } t^{(e)2} - Du^{(e)2} = m^2$$

ist.

II. Auf dieselbe Weise bestätigt man leicht, dass allgemein

$$t^{(e+1)} + t^{(e-1)} = \frac{2T}{m} t^{(e)}, \quad u^{(e+1)} + u^{(e-1)} = \frac{2T}{m} u^{(e)}$$

ist. Hieraus geht hervor, dass die beiden Reihen $t^0, t', t'', t''', \ldots, u^0, u', u'', u''', \ldots$ recurrente Reihen sind und die Beziehungsskala beider $\frac{2T}{m}, -1$ ist, nämlich:

$$t'' = \frac{2T}{m} t' - t^0, \quad t''' = \frac{2T}{m} t'' - t', \ldots; \quad u'' = \frac{2T}{m} u', \ldots.$$

Da es nun nach Voraussetzung irgend eine Form (M, N, P) mit der Determinante D giebt, in welcher $M, 2N, P$ durch m teilbar sind, so hat man:

$$T^2 = (N^2 - MP) U^2 + m^2,$$

und daher ist offenbar $4T^2$ durch m^2 teilbar. Mithin ist $\frac{2T}{m}$ eine ganze und zwar positive Zahl. Weil aber $t^0 = m$, $t' = T$, $u^0 = 0$, $u' = U$ und somit ganze Zahlen sind, so werden auch sämtliche Zahlen $t'', t''', \ldots, u'', u''', \ldots$ ganze Zahlen sein. Ferner ist ersichtlich, da $T^2 > m^2$ ist, dass alle $t^0, t', t'', t''', \ldots$ positiv sind und beständig bis ins Unendliche zunehmen ebenso alle $u^0, u', u'', u''' \ldots$

III. Nehmen wir an, dass es noch andere positive Werte von t, u gebe, welche nicht in der Reihe $t^0, t', t'', \ldots, u^0, u', u'', \ldots$ enthalten sind, etwa $\mathfrak{T}, \mathfrak{U}$, so wird offenbar, da die Reihe $u^0, u', \ldots$ von 0 bis ins Unendliche, wächst, $\mathfrak{U}$ notwendig zwischen zwei benachbarten Gliedern $u^{(n)}$ und $u^{(n+1)}$ liegen, so dass $\mathfrak{U} > u^{(n)}$ und $\mathfrak{U} < u^{(n+1)}$ ist. Um die Absurdität dieser Annahme zu beweisen, bemerken wir,

1. dass der Gleichung $t^2 - Du^2 = m^2$ auch genügt werden wird, wenn man setzt:

$$t = \frac{1}{m}(\mathfrak{T} t^{(n)} - D\mathfrak{U} u^{(n)}), \quad u = \frac{1}{m}(\mathfrak{U} t^{(n)} - \mathfrak{T} u^{(n)}).$$

Dies lässt sich leicht durch einfache Substitution bestätigen; dass aber diese Werte, welche wir der Kürze halber gleich τ, υ setzen, immer ganze Zahlen sind, beweisen wir folgendermassen. Wenn (M, N, P) eine Form mit der Determinante D und m der grösste gemeinschaftliche Teiler der Zahlen $M, 2N, P$ ist, so wird sowohl $\mathfrak{T} + N\mathfrak{U}$ als auch $t^{(n)} + Nu^{(n)}$ und daher auch $\mathfrak{U}(t^{(n)} + Nu^{(n)}) - u^{(n)}(\mathfrak{T} + N\mathfrak{U})$ oder $\mathfrak{U} t^{(n)} - \mathfrak{T} u^{(n)}$ durch m teilbar sein. Daher ist υ und somit auch τ eine ganze Zahl, da $\tau^2 = D\upsilon^2 + m^2$ ist.

2. Offenbar kann υ nicht gleich Null sein, denn hieraus würde folgen:

$$\mathfrak{U}^2 t^{(n)2} = \mathfrak{T}^2 u^{(n)2},$$

oder

$$\mathfrak{U}^2 (Du^{(n)2} + m^2) = u^{(n)2}(D\mathfrak{U}^2 + m^2)$$

oder $\mathfrak{U}^2 = u^{(n)2}$, im Widerspruch mit der Voraussetzung, nach welcher $\mathfrak{U} > u^{(n)}$ ist. Da nun abgesehen vom Werte 0 der kleinste Wert von u gleich U ist, so ist $\mathfrak{u}$ sicher nicht kleiner als U.

3. Aus den Werten von $t^{(n)}$, $t^{(n+1)}$, $u^{(n)}$, $u^{(n+1)}$ kann man leicht bestätigen, dass

$$mU = u^{(n+1)}\, t^{(n)} - t^{(n+1)}\, u^{(n)}$$

ist. Daher ist $\mathfrak{U}t^{(n)} - \mathfrak{T}u^{(n)}$ sicher nicht kleiner als $u^{(n+1)}\, t^{(n)} - t^{(n+1)}\, u^{(n)}$.

4. Nun erhält man aus der Gleichung $\mathfrak{T}^2 - D\mathfrak{U}^2 = m^2$:

$$\frac{\mathfrak{T}}{\mathfrak{U}} = \sqrt{D + \frac{m^2}{\mathfrak{U}^2}}$$

und analog:

$$\frac{t^{(n+1)}}{u^{(n+1)}} = \sqrt{D + \frac{m^2}{u^{(n+1)2}}},$$

woraus leicht folgt, dass $\frac{\mathfrak{T}}{\mathfrak{U}} > \frac{t^{(n+1)}}{u^{(n+1)}}$ ist. Hieraus aber und aus der Folgerung in 3) ergiebt sich:

$$(\mathfrak{U}t^{(n)} - \mathfrak{T}u^{(n)})\left(t^{(n)} + u^{(n)}\frac{\mathfrak{T}}{\mathfrak{U}}\right) > (u^{(n+1)}\, t^{(n)} - t^{(n+1)}\, u^{(n)})\left(t^{(n)} + u^{(n)}\frac{t^{(n+1)}}{u^{(n+1)}}\right),$$

oder wenn man die Entwicklung macht und für $\mathfrak{T}^2$, $t^{(n)2}$, $t^{(n+1)2}$ ihre Werte $D\mathfrak{U}^2 + m^2$, $Du^{(n)2} + m^2$, $Du^{(n+1)2} + m^2$ substituiert:

$$\frac{1}{\mathfrak{U}}(\mathfrak{U}^2 - u^{(n)2}) > \frac{1}{u^{(n+1)}}(u^{(n+1)2} - u^{(n)2}),$$

woraus, da jede Grösse offenbar positiv ist, durch Transposition folgt: $\mathfrak{U} + \frac{u^{(n)2}}{u^{(n+1)}} > u^{(n+1)} + \frac{u^{(n)2}}{\mathfrak{U}}$. Dies ist aber absurd, da der erste Teil der ersten Grösse kleiner ist als der erste Teil der zweiten und ebenso der zweite Teil jener kleiner als der zweite Teil dieser. Daher kann unsere Annahme nicht stattfinden, und die Reihen t^0, t', t'', ..., u^0, u', u'', ... stellen sämtliche positiven Werte von t, u dar.

Beispiel. Für $D = 61$, $m = 2$ fanden wir als kleinste positive Werte von t, u die folgenden: 1523, 195. Daher werden sämtliche positiven Werte dargestellt durch folgende Formeln:

$$t = \left(\frac{1523}{2} + \frac{195}{2}\sqrt{61}\right)^e + \left(\frac{1523}{2} - \frac{195}{2}\sqrt{61}\right)^e$$

$$u = \frac{1}{\sqrt{61}}\left[\left(\frac{1523}{2} + \frac{195}{2}\sqrt{61}\right)^e - \left(\frac{1523}{2} - \frac{195}{2}\sqrt{61}\right)^e\right].$$

Man findet aber:

$t^0 = 2,\ t' = 1523,\ t'' = 1523\,t' - t^0 = 2319527,\ t''' = 1523\,t'' - t' = 3532618098, \ldots$
$u^0 = 0,\ u' = 195,\ u'' = 1523u' - u^0 = 296985,\ u''' = 1523u'' - u' = 452307960, \ldots$

201.

Über das im vorigen Artikel behandelte Problem fügen wir noch folgende Bemerkungen hinzu:

1. Nachdem wir gezeigt haben, wie man die Gleichung $t^2 - Du^2 = m^2$, wo m der grösste gemeinschaftliche Teiler dreier Zahlen M, $2N$, P von solcher Beschaffenheit ist, dass $N^2 - MP = D$ ist, für alle Fälle lösen kann, verlohnt es der Mühe, alle Zahlen, welche solche Teiler sein können, oder alle Werte von m für einen gegebenen Wert von D zu bestimmen. Man setze $D = n^2D'$, so dass D' von quadratischen Factoren gänzlich frei ist, was erreicht wird, wenn man für n^2 das grösste in D aufgehende Quadrat nimmt; ist aber D schon an und für sich durch keinen quadratischen Factor teilbar, so müsste $n = 1$ gesetzt werden. Dann wird behauptet:

Erstens: Wenn D' von der Form $4k + 1$ ist, so ist jeder Teiler von $2n$ ein Wert von m und umgekehrt. Denn wenn g ein Teiler von $2n$ ist, so erhält man die Form $(g, n, \frac{n^2(1 - D')}{g})$, deren Determinante gleich D ist und in welcher offenbar der grösste gemeinschaftliche Teiler der Zahlen $g, 2n, \frac{n^2(D' - 1)}{g}$ gleich g ist (denn offenbar ist $\frac{n^2(D'-1)}{g^2} = \frac{4n^2}{g^2} \cdot \frac{D'-1}{4}$ eine ganze Zahl). Wenn aber umgekehrt angenommen wird, dass g ein Wert von m ist, nämlich der grösste gemeinschaftliche Teiler der Zahlen M, $2N$, P und $N^2 - MP = D$, so wird offenbar $4D$ oder $4n^2D'$ durch g^2 teilbar sein. Hieraus aber folgt, dass notwendig $2n$ durch g teilbar ist. Denn wenn g nicht in $2n$ aufginge, so würden g und $2n$ einen grössten gemeinschaftlichen Teiler haben, der kleiner als g wäre, und wenn dieser gleich δ und $2n = \delta n'$, $g = \delta g'$ gesetzt würde, so würde $n'^2 D'$ durch g'^2 teilbar, n' zu g' und daher auch n'^2 zu g'^2 prim und somit auch D' durch g'^2 teilbar sein, im Widerspruch mit der Voraussetzung, nach welcher D' von jedem quadratischen Factor befreit ist.

Zweitens: Wenn D' von der Form $4k + 2$ oder $4k + 3$ ist, so ist jeder Teiler von n ein Wert von m und umgekehrt, jeder Wert von m geht auch in n auf. Denn wenn g ein Teiler von n ist, so erhält man die Form $\left(g, 0, -\frac{n^2D'}{g}\right)$, deren Determinante gleich D und in der offenbar der grösste gemeinschaftliche Teiler der Zahlen $g, 0, \frac{n^2D'}{g}$ gleich g ist. — Nimmt man aber an, dass g ein Wert von m sei, nämlich der grösste gemeinschaftliche Teiler der Zahlen M, $2N$, P und $N^2 - MP = D$, so geht ebenso wie oben

g in $2n$ auf, oder $\frac{2n}{g}$ ist eine ganze Zahl. Wenn dieser Quotient ungerade wäre, würde das Quadrat $\frac{4n^2}{g^2} \equiv 1$ (mod. 4) und daher $\frac{4n^2D'}{g^2}$ entweder $\equiv 2$ oder $\equiv 3$ (mod. 4) sein. Nun ist aber $\frac{4n^2D'}{g^2} = \frac{4D}{g^2} = \frac{4N^2}{g^2} - \frac{4MP}{g^2} \equiv \frac{4N^2}{g^2}$ (mod. 4) und somit $\frac{4N^2}{g^2}$ entweder $\equiv 2$ oder $\equiv 3$ (mod. 4). Dies ist aber absurd, da jedes Quadrat entweder der Null oder der Einheit nach dem Modul 4 congruent sein muss. Daher ist der Quotient $\frac{2n}{g}$ notwendig gerade und somit $\frac{n}{g}$ eine ganze Zahl oder g ein Teiler von n.

Es geht hieraus also hervor, dass 1 immer ein Wert von m ist oder dass die Gleichung $t^2 - Du^2 = 1$ für jeden positiven nichtquadratischen Wert von D nach dem Vorhergehenden lösbar ist; dass ferner 2 nur dann ein Wert von m ist, wenn D entweder von der Form $4k$ oder von der Form $4k+1$ ist.

2. Ist $m > 2$, aber doch eine passende Zahl, so lässt sich die Lösung der Gleichung $t^2 - Du^2 = m^2$ auf die Lösung einer ähnlichen Gleichung zurückführen, in welcher m entweder 1 oder 2 ist. Setzt man wie vorher $D = n^2D'$, so wird, wenn m in n aufgeht, auch m^2 in D aufgehen. Nimmt man dann an, dass die kleinsten Werte von p, q in der Gleichung $p^2 - \frac{D}{m^2}q^2 = 1$ seien $p = P$, $q = Q$, so werden die kleinsten Werte von t, u in der Gleichung $t^2 - Du^2 = m^2$ sein: $t = mP$, $u = Q$. — Wenn aber m nicht in n aufgeht, so wird es wenigstens in $2n$ aufgehen und sicher gerade sein; $\frac{4D}{m^2}$ aber ist eine ganze Zahl. Und wenn dann als kleinste Werte von p, q in der Gleichung $p^2 - \frac{4D}{m^2}q^2 = 4$ die Werte $p = P$, $q = Q$ gefunden sind, so werden die kleinsten Werte von t, u in der Gleichung $t^2 - Du^2 = m^2$ lauten: $t = \frac{m}{2}P$, $u = Q$. — In beiden Fällen aber können nicht nur aus den kleinsten Werten von p, q die kleinsten Werte von t, u, sondern offenbar aus allen Werten jener alle Werte dieser nach dieser Methode abgeleitet werden.

3. Bezeichnen t^0, u^0; t', u'; t'', u'', ... sämtliche positiven Werte von t, u in der Gleichung $t^2 - Du^2 = m^2$, wie im vorigen Artikel, und trifft es sich, dass gewisse Werte aus jener Reihe den ersten Werten in derselben Reihe nach irgend welchem gegebenen Modul r congruent sind, z. B. $t^{(\rho)} \equiv t^0$ (oder $\equiv m$), $u^{(\rho)} \equiv u^0$ (oder $\equiv 0$) (mod. r), und zu gleicher Zeit die nächstfolgenden Werte den zweiten Werten, nämlich $t^{(\rho+1)} \equiv t'$, $u^{(\rho+1)} \equiv u'$ (mod. r), so ist auch:

$$t^{(\rho+2)} \equiv t'', \; u^{(\rho+2)} \equiv u''; \quad t^{(\rho+3)} \equiv t''', \; u^{(\rho+3)} \equiv u''', \ldots$$

Dies folgt leicht daraus, dass jede der beiden Reihen $t^0, t', t'', \ldots, u^0, u', u'', \ldots$ eine rekurrente Reihe ist; denn da

$$t'' = \frac{2T}{m} t' - t^0, \quad t^{(\rho+2)} = \frac{2T}{m} t^{(\rho+1)} - t^{(\rho)}$$

ist, so ist auch

$$t'' \equiv t^{(\rho+2)}$$

und ähnlich bei den übrigen. Hieraus aber folgt, dass allgemein

$$t^{(h+\rho)} \equiv t^h, \quad u^{(h+\rho)} \equiv u^h \pmod{r}$$

ist, wo h eine beliebige Zahl bezeichnet, und noch allgemeiner, dass, wenn

$$\mu \equiv \nu \pmod{\rho} \text{ ist, auch } t^{(\mu)} \equiv t^{(\nu)}, \quad u^{(\mu)} \equiv u^{(\nu)} \pmod{r} \text{ ist.}$$

4. Den in der vorigen Bemerkung geforderten Bedingungen kann aber stets genügt werden, es kann nämlich immer ein Index ρ (für irgend einen gegebenen Modul r) gefunden werden, für welchen

$$t^{(\rho)} \equiv t^0, \; t^{(\rho+1)} = t', \quad u^{(\rho)} \equiv u^0, \; u^{(\rho+1)} \equiv u'$$

ist. Um dies zu beweisen, bemerken wir:

Erstens, dass der dritten Bedingung immer genügt werden kann. Denn ohne Mühe erkennt man aus den in 1. angegebenen Kriterien, dass auch die Gleichung $p^2 - r^2Dq^2 = m^2$ lösbar ist, und wenn man annimmt, dass die kleinsten Werte von p, q (ausser m, o) P, Q seien, so werden sich unter den Werten von t, u offenbar auch $t = P, \; u = rQ$ befinden. Daher werden P, rQ in den Reihen $t^0, t', \ldots, u^0, u', \ldots$ enthalten sein, und wenn $P = t^{(\lambda)}, \; rQ = u^{(\lambda)}$ ist, so wird $u^{(\lambda)} \equiv 0 \equiv u^0 \pmod{r}$ sein. Ausserdem ist leicht ersichtlich, dass es zwischen u^0 und $u^{(\lambda)}$ kein Glied geben wird, welches u^0 nach dem Modul r congruent ist.

Zweitens ist klar, dass, wenn hier überdies die drei übrigen Bedingungen erfüllt sind, wenn nämlich auch $u^{(\lambda+1)} \equiv u', \; t^{(\lambda)} \equiv t^0, \; t^{(\lambda+1)} \equiv t'$ ist, nur $\rho = \lambda$ gesetzt zu werden braucht. Wenn aber eine oder die andere jener Bedingungen nicht stattfindet, so kann man, behaupte ich, sicher $\rho = 2\lambda$ setzen. Denn aus der Gleichung [1] und den allgemeinen Formeln für $t^{(e)}, \; u^{(e)}$ im vorhergehenden Artikel folgt:

$$t^{(2\lambda)} = \frac{1}{m}\left(t^{(\lambda)2} + Du^{(\lambda)2}\right) = \frac{1}{m}\left(m^2 + 2\,Du^{(\lambda)2}\right)$$

und daher:

$$\frac{t^{(2\lambda)} - t^0}{r} = \frac{2\,Du^{(\lambda)2}}{mr},$$

welche Grösse eine ganze Zahl ist, da nach Voraussetzung r in $u^{(\lambda)}$ und

ebenso m^2 in $4D$ und daher umsomehr m in $2D$ aufgeht. — Ferner ist $u^{(2\lambda)} = \frac{2}{m} t^{(\lambda)} u^{(\lambda)}$ und da

$$4t^{(\lambda)2} = 4Du^{(\lambda)2} + 4m^2$$

und daher durch m^2 teilbar ist, so ist auch $2t^{(\lambda)}$ teilbar durch m und somit $u^{(2\lambda)}$ teilbar durch r oder

$$u^{(2\lambda)} \equiv u^0 \pmod{r}.$$

Drittens findet man:

$$t^{(2\lambda+1)} = t' + \frac{2Du^{(\lambda)} u^{(\lambda+1)}}{m},$$

und da aus ähnlichem Grunde $\frac{2Du^{(\lambda)}}{mr}$ eine ganze Zahl ist, so wird:

$$t^{(2\lambda+1)} \equiv t' \pmod{r}.$$

Endlich findet man:

$$u^{(2\lambda+1)} = u' + \frac{2t^{(\lambda+1)} u^{(\lambda)}}{m},$$

und da $2t^{(\lambda+1)}$ durch m und $u^{(\lambda)}$ durch r teilbar ist, so ist:

$$u^{(2\lambda+1)} \equiv u' \pmod{r}.$$

Uebrigens wird der Nutzen der letzten beiden Bemerkungen im Folgenden zu Tage treten.

202.

Ein specieller Fall des Problems, nämlich die Auflösung der Gleichung $t^2 - Du^2 = 1$, ist bereits von den Mathematikern des vorigen Jahrhunderts behandelt worden. Der scharfsinnige Fermat legte dieses Problem den englischen Analysten vor, und Wallis nennt Brounker als Erfinder der Lösung, welche er in seiner *Algebra Kapitel 98* und *Opera, T. II. p. 418 u. ff.* anführt; Ozanam nennt als solchen Fermat und schliesslich Euler, der über sie in den *Comm. Petr. VI. p. 175, Comm. nov. XI. p. 28**), *Algebra, Pars II. p. 226, Opusc. An. I. p. 310* gehandelt hat, den Engländer Pell, weshalb jenes Problem von einigen Autoren das Pell'sche genannt worden ist. Alle diese Lösungen stimmen im Wesentlichen überein mit derjenigen, welche man erhält, wenn man im Artikel 198 diejenige reducierte Form anwendet, in welcher $a = 1$ ist. Dass aber die Operation, die sie vorschreiben, notwendig einmal ein Ende hat, oder dass das Problem immer wirklich lös-

*) In dieser Abhandlung ist der im Artikel 27 dargelegte Algorithmus durch ähnliche Zeichen dargestellt, was wir dort zu bemerken vergessen haben.

bar ist, hat vor Lagrange noch Niemand streng*) bewiesen, *Mélanges de la Soc. de Turin, T. IV. p. 19* und kürzer in *Hist. de l'Ac. de Berlin, 1767, p. 237.* Diese Untersuchung findet sich auch in den schon öfter angeführten Supplementen zu Euler's Algebra. Uebrigens bietet unsere Methode (die auf ganz verschiedenen Prinzipien beruht und nicht auf den Fall $m = 1$ beschränkt ist) meistens mehrere Wege dar, um zur Lösung zu gelangen, da wir ja im Artikel 198 von jeder beliebigen andern reducierten Form $(a, b, -a')$ ausgehen können.

203.

Aufgabe. Wenn die Formen Φ, φ, äquivalent sind, so soll man alle Transformationen der einen in die andere darstellen.

Auflösung. Wenn diese Formen nur auf eine einzige Weise (d. h. entweder nur eigentlich oder nur uneigentlich) äquivalent sind, so suche man nach Artikel 196 eine Transformation der Form φ in Φ, welche α, β, γ, δ sein möge; offenbar kann es andere als solche, welche mit dieser gleichartig sind, nicht geben. Wenn aber φ, Φ sowohl eigentlich als uneigentlich äquivalent sind, so suche man zwei ungleichartige Transformationen d. h. eine eigentliche und eine uneigentliche, etwa α, β, γ, δ und α', β', γ', δ', jede andere Transformation wird entweder mit dieser oder mit jener gleichartig sein. Wenn daher die Form φ gleich (a, b, c), ihre Determinante gleich D, der grösste gemeinschaftliche Teiler der Zahlen a, $2b$, c (wie immer im Vorhergehenden) gleich m ist und t, u unbestimmt alle der Gleichung $t^2 - Du^2 = m^2$ genügende Zahlen sind, so werden im ersteren Falle sämtliche Transformationen der Form φ in Φ unter I der folgenden Formeln, im letzteren entweder unter der ersten I oder unter der zweiten II enthalten sein.

$$\text{I.}\quad \begin{array}{ll} \frac{1}{m}[\alpha t - (\alpha b + \gamma c)u], & \frac{1}{m}[\beta t - (\beta b + \delta c)u] \\ \frac{1}{m}[\gamma t + (\alpha a + \gamma b)u], & \frac{1}{m}[\delta t + (\beta a + \delta b)u] \end{array}$$

$$\text{II.}\quad \begin{array}{ll} \frac{1}{m}[\alpha' t - (\alpha' b + \gamma' c)u], & \frac{1}{m}[\beta' t - (\beta' b + \delta' c)u] \\ \frac{1}{m}[\gamma' t + (\alpha' a + \gamma' b)u], & \frac{1}{m}[\delta' t + (\beta' a + \delta' b)u]. \end{array}$$

---

*) Was Wallis a. a. O. S. 427, 428 hierzu angiebt, hat kein Gewicht. Der Fehlschuss liegt darin, dass er S. 428 Z. 4 annimmt, dass, wenn eine Grösse p gegeben ist, ganze Zahlen z, a von der Beschaffenheit gefunden werden können, dass $\frac{z}{a}$ kleiner ist als p, der Unterschied aber kleiner ist als eine bestimmte Zahl. Dies ist jedenfalls richtig, wenn der bestimmte Unterschied eine gegebene Grösse ist, nicht aber, wenn er, wie es hier der Fall ist, von a und z abhängt und daher variabel ist.

Beispiel. Man will sämtliche Transformationen der Form (129, 92, 65) in die Form (42, 59, 81) haben. Dass diese nur uneigentlich äquivalent sind, haben wir im Artikel 195 gefunden und im folgenden Artikel haben wir die uneigentliche Transformation jener in diese $-47, -56, 73, 87$ ermittelt. Demnach werden alle Transformationen der Form (129, 92, 65) in die Form (42, 59, 81) dargestellt durch die Formel

$$-(47t+421u),\ -(56t+503u),\ 73t+653u,\ 87t+780u,$$

wo t, u unbestimmt alle der Gleichung $t^2-79u^2=1$ genügende Zahlen sind. Diese aber werden dargestellt durch die Formeln:

$$\pm t = \frac{1}{2}\left[(80+9\sqrt{79})^e+(80-9\sqrt{79})^e\right]$$

$$\pm u = \frac{1}{2\sqrt{79}}\left[(80+9\sqrt{79})^e-(80-9\sqrt{79})^e\right],$$

wo für e alle ganzen nicht negativen Zahlen zu nehmen sind.

204.

Es ist ersichtlich, dass die allgemeine sämtliche Transformationen darstellende Formel um so einfacher werden wird, je einfacher die anfängliche Transformation, aus welcher die Formel abgeleitet wurde, ist. Da es nun in unserm Belieben steht, von welcher Transformation wir ausgehen, so wird die allgemeine Formel häufig einfacher gemacht werden können, wenn wir aus der zuerst gefundenen Formel eine einfachere Transformation ableiten, indem wir t, u bestimmte Werte beilegen, und dann aus dieser eine andere Formel zusammensetzen. So geht z. B., wenn wir in der im vorigen Artikel gefundenen Formel $t=80$, $u=-9$ setzen, eine einfachere Transformation als die, von welcher wir ausgegangen waren, hervor, nämlich $29, 47, -37, -60$, woraus sich die allgemeine Formel ergiebt: $29t-263u,\ 47t-424u,\ -37t+337u,\ -60t+543u$. Wenn also nach den vorhergehenden Regeln eine allgemeine Formel aufgestellt ist, so wird man versuchen können, ob man nicht dadurch, dass man t, u bestimmte Werte $\pm t'$, $\pm u'$; $\pm t''$, $\pm u''$; ... beilegt, eine einfachere Formel erhält als die, aus welcher die Formel abgeleitet war, in welchem Falle aus jener Transformation sich eine einfachere Form ableiten lassen wird. — Übrigens bleibt bei der Entscheidung über die Einfachheit etwas Willkürliches übrig, das wir, wenn es sich der Mühe verlohnte, auf eine feste Norm zurückführen sowie auch in der Reihe t', u'; t'', u''; ... Grenzen angeben könnten, über welche hinaus die Transformationen beständig weniger einfach werden, so dass man nicht weiter fortzugehen, sondern nur innerhalb jener den Versuch anzustellen braucht. Da jedoch nach den von uns vorgeschriebenen Regeln die einfachste Transformation in den meisten Fällen entweder sofort oder bei Anwendung der Werte $\pm t'$, $\pm u'$

für t, u sich zu ergeben pflegt, so lassen wir diese Untersuchung der Kürze halber weg.

205.

Aufgabe. Alle Darstellungen einer gegebenen Zahl M durch die gegebene Form $ax^2 + 2bxy + cy^2$, deren positive nichtquadratische Determinante gleich D ist, zu finden.

Auflösung. Wir bemerken zunächst, dass die Ermittlung der Darstellungen durch zu einander nicht prime Werte von x, y hier in genau derselben Weise, wie oben (Artikel 181) für Formen mit negativer Determinante auf denjenigen Fall zurückgeführt werden kann, wo die Darstellungen durch zu einander prime Werte der Unbestimmten gesucht werden, so dass es unnütz sein würde, dies hier zu wiederholen. Für die Möglichkeit der Darstellungen durch zu einander prime Werte von x, y ist aber erforderlich, dass D quadratischer Rest von M sei, und wenn sämtliche Werte des Ausdrucks $\sqrt{D}$ (mod. M) lauten: $N, -N, N', -N', N'', -N'', \ldots$ (die man so annehmen darf, dass keiner grösser als $\frac{1}{2} M$ ist), so wird jede Darstellung der Zahl M durch die gegebene Form zu irgend einem dieser Werte gehören. Vor allem werden daher jene Werte ermittelt und sodann die zu den einzelnen gehörigen Darstellungen abgeleitet werden müssen. Darstellnngen, welche zum Werte N gehören, wird es nur geben, wenn die Formen (a, b, c) und $\left(M, N, \frac{N^2 - D}{M}\right)$ eigentlich äquivalent sind; ist dies der Fall, so suche man irgend eine eigentliche Transformation der ersteren in letztere, welche $\alpha, \beta, \gamma, \delta$ sein möge. Dann hat man als die zum Werte N gehörige Darstellung der Zahl M durch die Form (a, b, c) die folgende: $x = \alpha$, $y = \gamma$, und alle zu diesem Werte gehörende Darstellungen werden dargestellt durch die Formel:

$$x = \frac{1}{m}\,[\alpha t - (\alpha b + \gamma c)\,u], \quad y = \frac{1}{m}\,[\gamma t + (\alpha a + \gamma b)\,u],$$

wo m den grössten gemeinschaftllchen Teiler der Zahlen a, $2b$, c und t, u unbestimmt alle der Gleichung $t^2 - Du^2 = m^2$ genügenden Zahlen bezeichnen. — Übrigens wird diese allgemeine Formel offenbar um so einfacher werden, je einfacher die Transformation $\alpha, \beta, \gamma, \delta$ ist, aus der sie abgeleitet wurde; daher wird es nicht unnützlich sein, vorher nach dem vorigen Artikel die einfachste Transformation der Form (a, b, c) in $\left(M, N, \frac{N^2 - D}{M}\right)$ zu ermitteln und aus dieser die Formel abzuleiten. — Auf genau dieselbe Weise lassen sich die zu den übrigen Werten $-N, N', -N', \ldots$ gehörigen Darstellungen (wenn es deren giebt) durch allgemeine Formeln angeben.

Beispiel. Man sucht alle Darstellungen der Zahl 585 durch die Formel $42x^2 + 62xy + 21y^2$. Was die Darstellungen durch zu einander nicht prime

Werte von x, y anlangt, so ist sofort klar, dass es keine anderen dieser Art geben kann als solche, bei denen der grösste gemeinschaftliche Teiler von x, y gleich 3 ist, da 585 nur durch die eine Quadratzahl 9 teilbar ist. Wenn daher alle Darstellungen der Zahl $\frac{585}{9} = 65$ durch die Form $42x'^2 + 62x'y' + 21y'^2$, in denen x' zu y' prim ist, gefunden sind, so werden alle Darstellungen der Zahl 585 durch die Form $42x^2 + 62xy + 21y^2$, in denen x zu y nicht prim ist, erhalten werden, wenn man $x = 3x'$, $y = 3y'$ setzt. Die Werte des Ausdrucks $\sqrt{79}$ (mod. 65) sind ± 12, ± 27. Als Darstellung der Zahl 65, welche zum Werte -12 gehört, findet man: $x' = 2$, $y' = -1$; demnach werden alle zu diesem Werte gehörigen Darstellungen von 65 gegeben durch die Formel: $x' = 2t - 41u$, $y' = -t + 53u$, und somit alle hieraus entstehenden Darstellungen von 585 durch die Formel: $x = 6t - 123u$, $y = -3t + 159u$. In ähnlicher Weise findet man als allgemeine Formel, welche alle zum Werte $+12$ gehörigen Darstellungen von 65 ausdrückt, die folgende: $x' = 22t - 199u$, $y' = -23t + 211u$, und als Formel, welche sämtliche hieraus entstehende Darstellungen der Zahl 585 umfasst: $x = 66t - 597u$, $y = -69t + 633u$. Zu den Werten $+27$ und -27 aber gehört keine Darstellung der Zahl 65. — Um die Darstellungen der Zahl 585 durch zu einander prime Werte von x, y zu finden, muss man zunächst die Werte des Ausdrucks $\sqrt{79}$ (mod. 585) ermitteln, welche lauten: ± 77, ± 103, ± 157, ± 248. Man findet, dass zu den Werten ± 77, ± 103, ± 248 keine Darstellung gehört; zum Werte -157 aber gehört die Darstellung $x = 3$, $y = 1$, aus welcher man als allgemeine Formel, welche alle zu diesem Werte gehörige Darstellungen ergiebt, die folgende ableitet: $x = 3t - 114u$, $y = t + 157u$. Auf ähnliche Weise findet man als die zu $+157$ gehörige Darstellung: $x = 83$, $y = -87$ und als Formel, in welcher alle ähnlichen enthalten sind: $x = 83t - 746u$, $y = -87t + 789u$. Man erhält daher vier allgemeine Formeln, unter denen sämtliche Darstellungen der Zahl 585 durch die Form $42x^2 + 62xy + 21y^2$ enthalten sind, nämlich:

$$\begin{aligned}
x &= 6t - 123u, & y &= -3t + 159u \\
x &= 66t - 597u, & y &= -69t + 633u \\
x &= 3t - 114u, & y &= t + 157u \\
x &= 83t - 746u, & y &= -87t + 789u,
\end{aligned}$$

wobei t, u unbestimmt alle ganzen Zahlen bezeichnen, welche der Gleichung $t^2 - 79u^2 = 1$ genügen.

Bei speciellen Anwendungen der vorhergehenden Untersuchungen über Formen mit positiver nichtquadratischer Determinante halten wir uns der Kürze halber nicht auf, da sie jeder in analoger Weise wie in den Artikeln 176, 182 ohne Schwierigkeit von selbst wird machen können, und wenden uns sogleich zu den allein noch übrig bleibenden Formen mit positiver quadratischer Determinante.

Von den Formen mit quadratischer Determinante.

206.

Aufgabe. Wenn eine Form (a, b, c) mit der quadratischen Determinante h^2, wo h die positive Wurzel derselben bezeichnet, gegeben ist, so soll man eine ihr eigentlich äquivalente Form (A, B, C) finden, in welcher A zwischen den Grenzen 0 und $2h-1$ incl. liegt, $B=h$ und $C=0$ ist.

Auflösung. I. Da $h^2=b^2-ac$ ist, so wird $(h-b):a=c:-(h+b)$. Diesem Verhältnis sei das Verhältnis $\beta:\delta$ gleich, so dass β prim zu δ ist, und man bestimme α, γ so, dass $\alpha\delta-\beta\gamma=1$ ist, was möglich ist. Durch die Substitution α, β, γ, δ möge die Form (a, b, c) in (a', b', c') übergehen, die somit jener eigentlich äquivalent sein wird. Man erhält aber:

$$\begin{aligned} b' &= a\alpha\beta + b(\alpha\delta+\beta\gamma) + c\gamma\delta \\ &= (h-b)\alpha\delta + b(\alpha\delta+\beta\gamma) - (h+b)\beta\gamma \\ &= h(\alpha\delta-\beta\gamma) = h \\ c' &= a\beta^2 + 2b\beta\delta + c\delta^2 \\ &= (h-b)\beta\delta + 2b\beta\delta - (h+b)\beta\delta = 0. \end{aligned}$$

Wenn daher überdies a' bereits zwischen den Grenzen 0 und $2h-1$ liegt, so wird die Form (a', b', c') allen Bedingungen genügen.

II. Wenn aber a' ausserhalb der Grenzen 0 und $2h-1$ liegt, so sei A der kleinste positive Rest von a' nach dem Modul $2h$, welcher offenbar zwischen diesen Grenzen liegen wird, und man setze $A-a'=2hk$. Dann wird die Form (a', b', c') d. i. $(a', h, 0)$ durch die Substitution 1, 0, k, 1 übergehen in die Form $(A, h, 0)$, welche den Formen (a', b', c') und (a, b, c) eigentlich äquivalent ist und allen Bedingungen genügt. — Übrigens ist klar, dass die Form (a, b, c) in die Form $(A, h, 0)$ übergeht durch die Substitution: $\alpha+\beta k$, β, $\gamma+\delta k$, δ.

Beispiel. Gegeben sei die Form (27, 15, 8), deren Determinante gleich 9 ist. Hier ist $h=3$; ferner ist den Verhältnissen $-12:27=8:-18$ in kleinsten Zahlen das Verhältnis $4:-9$ gleich. Setzt man also $\beta=4$, $\delta=-9$, $\alpha=-1$, $\gamma=2$, so lautet hier die Form (a', b', c') folgendermassen: $(-1, 3, 0)$, und diese geht durch die Substitution 1, 0, 1, 1 über in die Form (5, 3, 0). Dies ist also die gesuchte Form, und die gegebene geht in sie über durch die eigentliche Substitution: 3, 4, -7, -9.

Derartige Formen (A, B, C), in welchen $C=0$, $B=h$ ist und in denen A zwischen den Grenzen 0 und $2h-1$ liegt, werden wir **reducierte** Formen nennen; dieselben sind also von den reducierten Formen mit negativer Determinante und von denen mit positiver nichtquadratischer Determinante wohl zu unterscheiden.

207.

Satz. Zwei nichtidentische reducierte Formen $(a, h, 0)$, $(a', h, 0)$ können nicht eigentlich äquivalent sein.

Beweis. Denn nimmt man an, dass sie eigentlich äquivalent seien, und geht die erstere in die letztere durch die eigentliche Substitution $\alpha, \beta, \gamma, \delta$ über, so hat man die vier Gleichungen:

[1] $$a\alpha^2 + 2h\alpha\gamma = a'$$
[2] $$a\alpha\beta + h(\alpha\delta + \beta\gamma) = h$$
[3] $$a\beta^2 + 2h\beta\delta = 0$$
[4] $$\alpha\delta - \beta\gamma = 1.$$

Multipliciert man die zweite Gleichung mit β, die dritte mit α und subtrahiert dann, so wird $-h(\alpha\delta - \beta\gamma)\beta = \beta h$ oder wegen [4]: $-\beta h = \beta h$, also notwendig $\beta = 0$. Daher folgt aus [4]: $\alpha\delta = 1$ und $\alpha = \pm 1$. Somit aus [1]: $a \pm 2h\gamma = a'$. Diese Gleichung kann aber nur bestehen, wenn $\gamma = 0$ (da nach Voraussetzung a und a' beide zwischen 0 und $2h$ liegen) d. h. wenn $a = a'$ ist oder die Formen $(a, h, 0)$ und $(a', h, 0)$ identisch sind, was gegen die Voraussetzung verstösst.

Hiernach lassen sich die folgenden **Aufgaben**, welche für nichtquadratische Determinanten bei weitem grössere Schwierigkeit bereiteten, ohne Mühe lösen.

I. Wenn zwei Formen F, F' mit derselben quadratischen Determinante gegeben sind, so soll man ermitteln, ob sie eigentlich äquivalent sind. Man suche zwei reducierte den Formen F, F' resp. eigentlich äquivalente Formen; sind diese identisch, so sind die gegebenen Formen eigentlich äquivalent, im andern Falle dagegen nicht.

II. Unter denselben Voraussetzungen soll man untersuchen, ob die Formen uneigentlich äquivalent sind. Es sei die der einen von beiden gegebenen Formen, z. B. der Form F, entgegengesetzte Form G; ist diese der Form F' eigentlich äquivalent, so werden F und F' uneigentlich äquivalent sein, und umgekehrt.

208.

Aufgabe. Wenn zwei eigentlich äquivalente Formen F, F' mit der Determinante h^2 gegeben sind, so soll man eine eigentliche Transformation der einen in die andere finden.

Auflösung. Der Form F sei die reducierte Form Φ eigentlich äquivalent, welche somit auch nach Voraussetzung der Form F' eigentlich äquivalent sein wird. Man suche nach Artikel 206 eine eigentliche Transformation der Form F in Φ, welche $\alpha, \beta, \gamma, \delta$ sein möge, ebenso eine eigentliche Transformation der Form F' in Φ, welche $\alpha', \beta', \gamma', \delta'$ sei. Dann wird Φ in F' durch die eigentliche Substitution $\delta', -\beta', -\gamma', \alpha'$ und hiernach F in F' durch die eigentliche Substitution

$$\alpha\delta' - \beta\gamma', \quad \beta\alpha' - \alpha\beta', \quad \gamma\delta' - \delta\gamma', \quad \delta\alpha' - \gamma\beta'$$

übergehen.

Es verlohnt der Mühe, für diese Transformation der Form F in F' eine andere Formel zu entwickeln, für welche man die reducierte Form Φ selbst nicht einmal zu kennen braucht. Wir nehmen an, es sei

$$F = (a, b, c), \quad F' = (a', b', c'), \quad \Phi = (A, h, 0).$$

Da den Verhältnissen $h - b : a$ oder $c : -(h + b)$ in kleinsten Zahlen das Verhältnis $\beta : \delta$ gleich ist, so sieht man leicht, dass $\frac{h-b}{\beta} = \frac{a}{\delta}$ eine ganze Zahl ist, welche gleich f sei; ebenso ist $\frac{c}{\beta} = \frac{-h-b}{\delta}$ eine ganze Zahl, welche gleich g sei. Man hat aber:

$$A = a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \text{ und daher } \beta A = a\alpha^2\beta + 2b\alpha\beta\gamma + c\beta\gamma^2$$

oder (wenn man $\delta(h - b)$ für $a\beta$ und βg für c setzt):

$$\beta A = \alpha^2\delta h + b(2\beta\gamma - \alpha\delta)\alpha + \beta^2\gamma^2 g$$

oder (wegen $b = -h - \delta g$):

$$\beta A = 2\alpha(\alpha\delta - \beta\gamma)h + (\alpha\delta - \beta\gamma)^2 g = 2\alpha h + g.$$

Ebenso:

$$\begin{aligned} \delta A &= a\alpha^2\delta + 2b\alpha\gamma\delta + c\gamma^2\delta \\ &= \alpha^2\delta^2 f + b(2\alpha\delta - \beta\gamma)\gamma - \beta\gamma^2 h \\ &= (\alpha\delta - \beta\gamma)^2 f + 2\gamma(\alpha\delta - \beta\gamma)h = 2\gamma h + f. \end{aligned}$$

Daher:

$$\alpha = \frac{\beta A - g}{2h}, \quad \gamma = \frac{\delta A - f}{2h}.$$

Setzt man in ganz derselben Weise:

$$\frac{h - b'}{\beta'} = \frac{a'}{\delta'} = f', \quad \frac{c'}{\beta'} = \frac{-h - b'}{\delta'} = g',$$

so wird:

$$\alpha' = \frac{\beta' A - g'}{2h}, \quad \gamma' = \frac{\delta' A - f'}{2h}.$$

Setzt man diese Werte von $\alpha, \gamma, \alpha', \gamma'$ in die eben angeführte Formel für die Transformation der Form F in F' ein, so geht sie über in die folgende:

$$\frac{\beta f' - \delta' g}{2h}, \quad \frac{\beta' g - \beta g'}{2h}, \quad \frac{\delta f' - \delta' f}{2h}, \quad \frac{\beta' f - \delta g'}{2h},$$

aus welcher A gänzlich verschwunden ist.

Wenn zwei uneigentlich äquivalente Formen F, F' gegeben sind und eine uneigentliche Transformation der einen in die andere gesucht wird, so sei die Form G der Form F entgegengesetzt und eine eigentliche Transformation der Form G in F' die folgende: α, β, γ, δ. Dann ist offenbar α, β, $-\gamma$, $-\delta$ eine uneigentliche Transformation der Form F in F'.

Schliesslich ist klar, dass, wenn die gegebenen Formen sowohl eigentlich als uneigentlich äquivalent sind, auf diese Weise zwei Transformationen, eine eigentliche und eine uneigentliche, gefunden werden können.

209.

Es bleibt daher nur noch übrig, zu zeigen, wie aus einer Transformation alle übrigen gleichartigen abgeleitet werden können. Dies hängt aber ab von der Lösung der unbestimmten Gleichung $t^2 - h^2u^2 = m^2$, wo m den grössten gemeinschaftlichen Teiler der Zahlen a, $2b$, c bezeichnet und (a, b, c) die eine der beiden äquivalenten Formen ist. Aber diese Gleichung lässt sich stets nur auf zwei Arten lösen, nämlich indem man entweder $t = m$, $u = 0$ oder $t = -m$, $u = 0$ setzt. Denn nehmen wir an, dass es noch eine andere Lösung $t = T$, $u = U$ gebe, so dass U nicht gleich Null ist, so wird, weil m^2 sicher in $4h^2$ aufgeht, $\frac{4T^2}{m^2} = \frac{4U^2h^2}{m^2} + 4$ und sowohl $\frac{4T^2}{m^2}$ als auch $\frac{4h^2U^2}{m^2}$ eine ganze Quadratzahl sein. Man sieht aber ohne Mühe, dass die Zahl 4 nur dann die Differenz zweier ganzer Quadratzahlen sein kann, wenn das kleinere Quadrat gleich Null d. h. $U = 0$ ist, was mit der Annahme im Widerspruch steht. — Wenn daher die Form F in die Form F' mittelst der Substitution α, β, γ, δ übergeht, so giebt es ausser der Transformation $-\alpha$, $-\beta$, $-\gamma$, $-\delta$ keine mit ihr gleichartige Transformation weiter. Wenn daher die beiden Formen entweder nur eigentlich oder nur uneigentlich äquivalent sind, so giebt es nur zwei Transformationen; sind sie aber sowohl eigentlich als auch uneigentlich äquivalent, so giebt es deren vier, nämlich zwei eigentliche und zwei uneigentliche.

210.

Satz. Wenn zwei reducierte Formen $(a, h, 0)$, $(a', h, 0)$ uneigentlich äquivalent sind, so wird $aa' \equiv m^2 \pmod{2mh}$, wo m den grössten gemeinschaftlichen Teiler der Zahlen a, $2h$ oder a', $2h$ bezeichnet, und umgekehrt, wenn a, $2h$ und a', $2h$ denselben grössten gemeinschaftlichen Teiler m haben, und $aa' \equiv m^2 \pmod{2mh}$ ist, so sind die Formen $(a, h, 0)$, $(a', h, 0)$ uneigentlich äquivalent.

Beweis. I. Es möge die Form $(a, h, 0)$ in die Form $(a', h, 0)$ durch die uneigentliche Substitution α, β, γ, δ übergehen, so dass man die vier Gleichungen hat:

[1] $$a\alpha^2 + 2h\alpha\gamma = a'$$
[2] $$a\alpha\beta + h(\alpha\delta + \beta\gamma) = h$$
[3] $$a\beta^2 + 2h\beta\delta = 0$$
[4] $$\alpha\delta - \beta\gamma = -1.$$

Hieraus folgt, wenn wir [4] mit h multiplicieren und von [2] subtrahieren, was wir kurz durch $[2] - h[4]$ ausdrücken:

[5] $$(a\alpha + 2h\gamma)\beta = 2h.$$

Analog folgt aus $\gamma\delta[2] - \gamma^2[3] - (a + a\gamma\beta + h\gamma\delta)[4]$, nachdem man weggelassen, was sich hebt:

[6] $$-a\alpha\delta = a + 2h\gamma\delta \text{ oder } -(a\alpha + 2h\gamma)\delta = a;$$

endlich aus $a[1]$: $a\alpha(a\alpha + 2h\gamma) = aa'$ oder:

$$(a\alpha + 2h\gamma)^2 - aa' = 2h\gamma(a\alpha + 2h\gamma)$$

oder:

[7] $$(a\alpha + 2h\gamma)^2 \equiv aa' [\text{mod. } 2h(a\alpha + 2h\gamma)].$$

Nun folgt aus [5] und [6], dass $a\alpha + 2h\gamma$ in $2h$ und a und daher auch in m, welches der grösste gemeinschaftliche Teiler von a und $2h$ ist, aufgeht; offenbar aber wird m auch in $a\alpha + 2h\gamma$ aufgehen; daher ist notwendig $a\alpha + 2h\gamma$ entweder $= +m$ oder gleich $-m$. Daher folgt aus [7] sofort: $m^2 \equiv aa'$ (med. $2mh$).

II. Wenn a, $2h$; a', $2h$ denselben grössten gemeinschaftlichen Teiler m haben und überdies $aa' \equiv m^2$ (mod. $2mh$) ist, so werden $\frac{a}{m}$, $\frac{2h}{m}$, $\frac{a'}{m}$, $\frac{aa'-m^2}{2mh}$ ganze Zahlen sein. Man bestätigt aber leicht, dass die Form $(a, h, 0)$ in die Form $(a', h, 0)$ durch die Substitution $-\frac{a'}{m}$, $-\frac{2h}{m}$, $\frac{aa'-m^2}{2mh}$, $\frac{a}{m}$ übergeht, und dass diese Transformation eine uneigentliche ist. Daher sind jene Formen uneigentlich äquivalent.

Hiernach kann man auch sogleich beurteilen, ob eine gegebene reducierte Form sich selbst uneigentlich äquivalent ist. Bezeichnet man nämlich den grössten gemeinschaftlichen Teiler der Zahlen a, $2h$ mit m, so muss $a^2 \equiv m^2$ (mod. $2mh$) sein.

211.

Alle reducierten Formen mit gegebener Determinante h^2 werden erhalten, wenn man in der unbestimmten Form $(A, h, 0)$ für A alle Zahlen von 0 bis $2h - 1$ einschliesslich substituiert; deren Anzahl ist somit gleich $2h$. Offenbar können sämtliche Formen mit der Determinante h^2 in ebenso viele **Klassen** verteilt werden, und diese werden dieselben Eigenschaften besitzen, welche wir oben (Artikel 175, 195) für die Klassen der Formen mit negativer und mit positiver nichtquadratischer Determinante erhalten haben. So werden z. B. alle Formen mit der Determinante 25 in

zehn Klassen zerfallen, welche nach den in jeder derselben enthaltenen reducierten Formen unterschieden werden können. Diese reducierten Formen sind: (0, 5, 0), (1, 5, 0), (2, 5, 0), (5, 5, 0), (8, 5, 0), (9, 5, 0), welche sich selbst zugleich uneigentlich äquivalent sind; (3, 5, 0), welcher (7, 5, 0), und (4, 5, 0), welcher (6, 5, 0) uneigentlich äquivalent ist.

212.

Aufgabe. Alle Darstellungen einer gegebenen Zahl M durch eine gegebene Form $ax^2 + 2bxy + cy^2$ mit der Determinante h^2 zu finden.

Die Auflösung dieser Aufgabe könnte aus den Prinzipien des Artikels 168 in genau derselben Weise abgeleitet werden, wie wir dies oben (Artikel 180, 181, 205) für Formen mit negativer und mit positiver nichtquadratischer Determinante gezeigt haben; da dies keiner Schwierigkeit unterliegt, würde es unnütz sein, dasselbe hier zu wiederholen. Dagegen wird es nicht überflüssig sein, die Lösung aus einem andern Prinzip, welches dem vorliegenden Falle eigentümlich ist, abzuleiten.

Setzt man wie in den Artikeln 206, 208:

$$h - b : a = c : -(h + b) = \beta : \delta$$
$$\frac{h-b}{\beta} = \frac{a}{\delta} = f; \quad \frac{c}{\beta} = \frac{-h-b}{\delta} = g,$$

so bestätigt man leicht, dass die gegebene Form das Product aus den Factoren $\delta x - \beta y$ und $fx - gy$ ist. Hieraus geht hervor, dass jede Darstellung der Zahl M durch die gegebene Form eine Zerlegung der Zahl M in zwei Factoren giebt. Wenn daher $d, d', d'', \ldots$ sämtliche Teiler der Zahl M sind (worunter auch 1 und M einzurechnen sind und jeder einzelne zweimal, nämlich sowohl positiv als negativ, zu nehmen ist), so werden offenbar alle Darstellungen der Zahl M erhalten, wenn man der Reihe nach setzt:

$$\delta x - \beta y = d, \quad fx - gy = \frac{M}{d}$$
$$\delta x - \beta y = d', \quad fx - gy = \frac{M}{d'}$$

u. s. w.,

die Werte von x und y hieraus entwickelt und diejenigen Darstellungen verwirft, in denen x oder y gebrochene Werte erhalten. Offenbar aber folgt aus den beiden ersten Gleichungen:

$$x = \frac{\beta M - gd^2}{(\beta f - \delta g)d}, \quad y = \frac{\delta M - fd^2}{(\beta f - \delta g)d},$$

und dass diese Werte immer b e s t i m m t sind, geht daraus hervor, dass $\beta f - \delta g = 2h$ und daher der Nenner sicher nicht gleich Null ist. — Übrigens hätten aus demselben Prinzipe, nämlich dass sich jede Form mit quadra-

tischer Determinante in zwei Factoren zerlegen lässt, auch die übrigen Probleme gelöst werden können; doch wollten wir uns auch hier lieber einer analogen Methode bedienen, wie diejenige ist, welche wir oben für die Formen mit nichtquadratischer Determinante angegeben haben.

Beispiel. Gesucht werden sämtliche Darstellungen der Zahl 12 durch die Form $3x^2 + 4xy - 7y^2$. Diese zerfällt in die Factoren $x - y$ und $3x + 7y$. Sämtliche Teiler der Zahl 12 sind $\mp 1, 2, 3, 4, 6, 12$. Setzt man $x - y = 1$, $3x + 7y = 12$, so folgt $x = \frac{19}{10}$, $y = \frac{9}{10}$, welche Werte, weil gebrochen, zu verwerfen sind. Ebenso erhält man aus den Teilern $-1, \pm 3, \pm 4, \pm 6, \pm 12$ unbrauchbare Werte. Aus dem Teiler $+2$ aber erhält man die Werte $x = 2$, $y = 0$, und aus dem Teiler -2 die folgenden $x = -2$, $y = 0$. Ausser diesen beiden Darstellungen giebt es daher keine weiter.

Diese Methode lässt sich nicht anwenden, wenn $M = 0$ ist. Denn offenbar müssen in diesem Falle sämtliche Werte von x, y entweder der Gleichung $\delta x - \beta y = 0$ oder der Gleichung $fx - gx = 0$ genügen. Sämtliche Lösungen der ersten Gleichung aber sind enthalten in der Formel $x = \beta z$, $y = \delta z$, wenn z unbestimmt irgend eine ganze Zahl bezeichnet (wofern, wie vorausgesetzt wird, β, δ prim zu einander sind), und ebenso werden, wenn man den grössten gemeinschaftlichen Teiler der Zahlen f und g gleich m setzt, sämtliche Lösungen der letzteren Gleichung dargestellt durch die Formel $x = \frac{gz}{m}$, $y = \frac{fz}{m}$. Daher umfassen diese beiden allgemeinen Formeln sämtliche Darstellungen der Zahl M in diesem Falle.

Im Vorhergehenden haben wir Alles, was auf die Erkennung der Äquivalenz und auf die Auffindung sämtlicher Transformationen der Formen sowie auf die Ermittlung sämtlicher Darstellungen gegebener Zahlen durch gegebene Formen Bezug hat, in einer Weise auseinandergesetzt, dass nichts weiter zu wünschen sein dürfte. Es bleibt daher nur noch übrig, zu zeigen, wie man, wenn zwei Formen gegeben sind, welche wegen der **Ungleichheit ihrer Determinanten** nicht äquivalent sein können, entscheiden kann, ob nicht die eine unter der andern enthalten ist, und wenn dies der Fall ist, wie man sämtliche Transformationen jener in diese finden kann.

Formen, welche unter andern enthalten und trotzdem diesen nicht äquivalent sind.

213.

Wir haben oben in den Artikeln 157, 158 gezeigt, dass, wenn die Form f mit der Determinante D die Form F mit der Determinante E enthält und in dieselbe durch die Substitution α, β, γ, δ übergeht, $E = (\alpha\delta - \beta\gamma)^2 D$ ist; dass ferner, wenn $\alpha\delta - \beta\gamma = \pm 1$ ist, die Form f die

Form F nicht nur enthält, sondern ihr auch äquivalent ist und dass demzufolge, wenn f die Form F zwar enthält, ihr aber nicht äquivalent ist, der Quotient $\frac{E}{D}$ eine die Einheit übersteigende ganze Zahl ist. Es wird daher hier die Aufgabe zu lösen sein, zu entscheiden, ob eine gegebene Form f mit der Determinante D eine gegebene Form F mit der Determinante De^2 enthält, wobei angenommen wird, dass e eine positive ganze Zahl grösser als 1 ist. Diese Aufgabe erledigen wir in der Weise, dass wir zeigen, wie man die endliche Anzahl der unter f enthaltenen Formen von der Beschaffenheit bestimmen kann, dass, wenn die Form F unter f enthalten ist, sie notwendig irgend einer von jenen äquivalent sein muss.

I. Wir nehmen an, dass sämtliche (positive) Teiler der Zahl e (einschliesslich 1 und e) seien: $m, m', m'', \ldots$ und dass $e = mn = m'n' = m''n'' \ldots$ sei. Der Kürze wegen bezeichnen wir die Form, in welche f durch die eigentliche Substitution $m, 0, 0, n$ übergeht, mit $(m; 0)$, die Form, in welche f durch die eigentliche Substitution $m, 1, 0, n$ übergeht, mit $(m; 1)$ u. s. w. und allgemein die Form, in welche f durch die eigentliche Substitution $m, k, 0, n$ übergeht, mit $(m; k)$. In analoger Weise möge f durch die eigentliche Substitution $m', 0, 0, n'$ in $(m'; 0)$, durch $m', 1, 0, n'$ in $(m'; 1)$, u. s. w., durch $m'', 0, 0, n''$ in $(m''; 0)$ u. s. w. u. s. w. übergehen. Alle diese Formen sind unter f eigentlich enthalten, und die Determinante einer jeden ist gleich De^2. Den Complex aller Formen $(m; 0)$, $(m; 1)$, $(m; 2), \ldots, (m; m-1)$; $(m'; 0)$, $(m'; 1), \ldots, (m'; m'-1)$; $(m''; 0), \ldots$, deren Anzahl gleich $m + m' + m'' + \cdots$ ist, und die, wie man leicht sieht, alle von einander verschieden sind, bezeichnen wir mit Ω.

Wenn z. B. f die folgende Form: (2, 5, 7) und $e = 5$ ist, so wird Ω die folgenden sechs Formen umfassen: (1; 0), (5; 0), (5; 1), (5; 2), (5; 3), (5; 4), und diese lauten entwickelt: (2, 25, 175), (50, 25, 7), (50, 35, 19), (50, 45, 35), (50, 55, 55), (50, 65, 79).

II. Ich behaupte nun, dass, wenn die Form F mit der Determinante De^2 unter f eigentlich enthalten ist, dieselbe notwendig irgend einer der Formen Ω eigentlich äquivalent ist. Denn nehmen wir an, dass die Form f in F übergehe durch die eigentliche Substitution $\alpha, \beta, \gamma, \delta$, so ist $\alpha\delta - \beta\gamma = e$. Es sei ferner der grösste gemeinschaftliche positiv genommene Teiler der Zahlen γ, δ (welche nicht beide gleich 0 sein können) gleich n und $\frac{e}{n} = m$, welches offenbar eine ganze Zahl ist. Man nehme g, h so an, dass $\gamma g + \delta h = n$ ist, und endlich sei k der kleinste positive Rest der Zahl $\alpha g + \beta h$ nach dem Modul m. Dann wird die Form $(m; k)$, welche offenbar unter den Formen Ω enthalten ist, der Form F eigentlich äquivalent sein und zwar wird sie in dieselbe übergehen durch die eigentliche Substitution:

$$\frac{\gamma}{n}\cdot\frac{\alpha g + \beta h - k}{m} + h,\quad \frac{\delta}{n}\cdot\frac{\alpha g + \beta h - k}{m} - g,\quad \frac{\gamma}{n},\quad \frac{\delta}{n}.$$

Denn **zunächst** ist klar, dass diese vier Zahlen ganze Zahlen sind; **sodann** bestätigt man leicht, dass die Substitution eine eigentliche ist; **endlich** ist offenbar die Form, in welche $(m; k)$ durch jene Substitution übergeht, dieselbe wie die, in welche f*) übergeht durch die Substitution:

$$m\left(\frac{\gamma}{n}\cdot\frac{\alpha g+\beta h-k}{m}+h\right)+\frac{k\gamma}{n},\quad m\left(\frac{\delta}{n}\cdot\frac{\alpha g+\beta h-k}{m}-g\right)+\frac{k\delta}{n},\ \gamma,\ \delta,$$

oder, da $mn=e=\alpha\delta-\beta\gamma$ und daher $\beta\gamma+mn=\alpha\delta$, $\alpha\delta-mn=\beta\gamma$ ist, durch die folgende:

$$\frac{1}{n}(\alpha\gamma g+\alpha\delta h),\quad \frac{1}{n}(\beta\gamma g+\beta\delta h),\ \gamma,\ \delta,$$

oder schliesslich, da $\gamma g+\delta h=n$ ist, durch die folgende α, β, γ, δ, d. h. nach Voraussetzung in F. Demnach sind $(m; k)$ und F eigentlich äquivalent.

Hiernach lässt sich also immer entscheiden, ob irgend eine gegebene Form f mit der Determinante D die Form F mit der Determinante De^2 eigentlich enthält. Fragt man aber, ob f die Form F uneigentlich enthält, so braucht man nur zu untersuchen, ob die zu F entgegengesetzte Form unter f eigentlich enthalten ist (Artikel 159).

214.

Aufgabe. Wenn zwei Formen, f mit der Determinante D und F mit der Determinante De^2, gegeben sind, von denen die erstere die letztere eigentlich enthält, so soll man alle eigentlichen Transformationen der Form f in F darstellen.

Auflösung. Bezeichnet Ω denselben Formencomplex wie im vorigen Artikel, so suche man aus diesem Complex alle Formen heraus, welchen F eigentlich äquivalent ist; dieselben seien Φ, Φ', Φ'', ... Jede dieser Formen giebt in folgender Weise eigentliche Transformationen der Form f in F und zwar jede einzelne wieder andere, alle zusammen aber sämtliche (d. h. es giebt keine eigentliche Transformation der Form f in F, welche nicht von einer der Formen Φ, Φ', ... geliefert würde). Da das Verfahren für alle Formen Φ, Φ', ... dasselbe ist, so sprechen wir nur von einer derselben.

Wir nehmen an, dass $\Phi=(M; K)$ und $e=MN$ sei, so dass f in Φ durch die eigentliche Substitution M, K, 0, N übergeht. Ferner bezeichnen wir sämtliche eigentlichen Transformationen der Form Φ in F unbestimmt mit $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$. Dann wird f in Φ offenbar durch die eigentliche Substitution $M\mathfrak{a}+K\mathfrak{c}$, $M\mathfrak{b}+K\mathfrak{d}$, $N\mathfrak{c}$, $N\mathfrak{d}$ übergehen, und auf diese Weise wird aus jeder eigentlichen Transformation der Form Φ in F eine eigentliche Transformation der Form f in F hervorgehen. — In derselben Weise sind die

*) Die nämlich durch die Substitution $(m, k, 0, n)$ in $(m; k)$ übergeht. Vgl. Artikel 159.

übrigen Formen Φ', Φ'', ... zu behandeln, deren einzelne eigentliche Transformationen in F eine eigentliche Transformation der Form f in F liefern.

Damit klar werde, dass diese Auflösung in jeder Beziehung vollständig ist, ist zu zeigen:

I. Dass auf diese Weise alle möglichen eigentlichen Transformationen der Form f in F erhalten werden. Es sei α, β, γ, δ irgend eine eigentliche Transformation der Form f in F und wie in II des vorigen Artikels n der grösste gemeinschaftliche Teiler der Zahlen γ, δ; die Zahlen m, g, h, k aber seien auf dieselbe Weise wie dort bestimmt. Dann wird $(m; k)$ sich unter den Formen Φ, Φ', ... befinden und

$$\frac{\gamma}{n}\cdot\frac{\alpha g+\beta h-k}{m}+h,\quad \frac{\delta}{n}\cdot\frac{\alpha g+\beta h-k}{m}-g,\quad \frac{\gamma}{n},\quad \frac{\delta}{n}$$

irgend eine der eigentlichen Transformationen dieser Form in F sein; aus dieser aber erhält man nach der eben angegebenen Regel die Transformation α, β, γ, δ. Dies Alles ist im vorigen Artikel bewiesen.

II. Dass alle auf diese Weise sich ergebenden Transformationen verschieden sind, oder dass keine zweimal erhalten wird. Man erkennt zwar ohne Mühe, dass mehrere verschiedene Transformationen derselben Form Φ oder Φ' u. s. w. in F nicht dieselbe Transformation der Form f in F hervorbringen können; dass aber auch nicht verschiedene Formen, etwa Φ und Φ', dieselbe Transformation liefern können, wird so bewiesen. Wir nehmen an, dass die eigentliche Transformation α, β, γ, δ der Form f in F sowohl aus der eigentlichen Transformation $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$ der Form Φ in F als auch aus der eigentlichen Transformation $\mathfrak{a}'$, $\mathfrak{b}'$, $\mathfrak{c}'$, $\mathfrak{d}'$ der Form Φ' in F erhalten werde. Ferner sei $\Phi = (M; K)$, $\Phi' = (M'; K')$; $e = MN = M'N'$. Dann hat man die Gleichungen:

$$[1]\qquad \alpha = M\mathfrak{a} + K\mathfrak{c} = M'\mathfrak{a}' + K'\mathfrak{c}'$$
$$[2]\qquad \beta = M\mathfrak{b} + K\mathfrak{d} = M'\mathfrak{b}' + K'\mathfrak{d}'$$
$$[3]\qquad \gamma = N\mathfrak{c} = N'\mathfrak{c}'$$
$$[4]\qquad \delta = N\mathfrak{d} = N'\mathfrak{d}'$$
$$[5]\qquad \mathfrak{a}\mathfrak{d} - \mathfrak{b}\mathfrak{c} = \mathfrak{a}'\mathfrak{d}' - \mathfrak{b}'\mathfrak{c}' = 1.$$

Aus $\mathfrak{a}\,[4] - \mathfrak{b}\,[3]$ folgt mit Hülfe der Gleichung [5]: $N = N'(\mathfrak{a}\mathfrak{d}' - \mathfrak{b}\mathfrak{c}')$, daher geht N' in N auf; analog folgt aus $\mathfrak{a}'[4] - \mathfrak{b}'[3]$: $N(\mathfrak{a}'\mathfrak{d} - \mathfrak{b}'\mathfrak{c}) = N'$, mithin geht N in N' auf; folglich ist, weil sowohl N als N' als positiv vorausgesetzt werden, notwendig $N = N'$ und $M = M'$ und hiernach zufolge [3] und [4]: $\mathfrak{c} = \mathfrak{c}'$, $\mathfrak{d} = \mathfrak{d}'$. Ferner folgt aus $\mathfrak{a}\,[2] - \mathfrak{b}\,[1]$:

$$K = M'(\mathfrak{a}\mathfrak{b}' - \mathfrak{b}\mathfrak{a}') + K'(\mathfrak{a}\mathfrak{d}' - \mathfrak{b}\mathfrak{c}') = M(\mathfrak{a}\mathfrak{b}' - \mathfrak{b}\mathfrak{a}') + K',$$

somit $K \equiv K' \pmod{M}$, und dies ist nur möglich, wenn $K = K'$ ist, da sowohl K als K' zwischen den Grenzen 0 und $M-1$ liegt. Demnach sind die Formen im Widerspruch mit der Voraussetzung nicht verschieden.

Übrigens ist klar, dass, wenn D negativ oder positiv quadratisch ist, nach dieser Methode alle eigentlichen Transformationen der Form f in F wirklich gefunden werden können; wenn aber D eine positive nichtquadratische Zahl ist, so werden gewisse allgemeine Formeln angegeben werden können, in welchen alle eigentlichen Transformationen (deren Anzahl unendlich gross ist) enthalten sind.

Schliesslich werden, wenn die Form F uneigentlich unter der Form f enthalten ist, alle uneigentlichen Transformationen jener in diese nach der angegebenen Methode leicht dargestellt werden können. Wenn nämlich α, β, γ, δ unbestimmt alle eigentlichen Transformationen der Form f in die Form, welche der Form F entgegengesetzt ist, bezeichnen, so werden sämtliche uneigentlichen Transformationen der Form f in F dargestellt durch $\alpha, -\beta, \gamma, -\delta$.

Beispiel. Man will alle Transformationen der Form (2, 5, 7) in (275, 0, — 1), welche sowohl eigentlich als uneigentlich unter jener enthalten ist, haben. Den Complex der Formen Ω für diesen Fall haben wir schon im vorigen Artikel angegeben; eine genaue Untersuchung ergiebt, dass sowohl (5; 1) als auch (5; 4) der Form (275, 0, — 1) eigentlich äquivalent sind. Nach der oben entwickelten Theorie findet man, dass sämtliche eigentlichen Transformationen der Form (5; 1) d. i. (50, 35, 19) in (275, 0, — 1) unter der allgemeinen Formel enthalten sind:

$$16t - 275u, \quad -t + 16u, \quad -15t + 275u, \quad t - 15u,$$

wo t, u unbestimmt alle ganzen der Gleichung $t^2 - 275\,u^2 = 1$ genügenden Zahlen bezeichnen. Daher werden sämtliche hieraus sich ergebende eigentliche Transformationen der Form (2, 5, 7) in die Form (275, 0, — 1) enthalten sein unter der allgemeinen Formel:

$$65t - 1100u, \quad -4t + 65u, \quad -15t + 275\,u, \quad t - 15u.$$

In analoger Weise sind sämtliche eigentlichen Transformationen der Form (5; 4) d. h. der Form (50, 65, 79) in die Form (275, 0, — 1) enthalten in der allgemeinen Formel:

$$14t + 275u, \quad t + 14u, \quad -15t - 275u, \quad -t - 15u,$$

und daher alle eigentlichen Transformationen der Form (2, 5, 7) in die Form (275, 0, — 1), welche daraus entstehen, unter der folgenden:

$$10t + 275u, \quad t + 10u, \quad -15t - 275\,u, \quad -t - 15u.$$

Diese beiden Formeln umfassen also alle gesuchten eigentlichen Transformationen.*) — In derselben Weise aber findet man, dass sämtliche uneigent-

*) Kürzer werden alle eigentlichen Transformationen dargestellt durch die Formel:

$$10t + 55u, \quad t + 2u, \quad -15\,t - 55\,u, \quad -t - 3u,$$

wo t, u unbestimmt alle der Gleichung $t^2 - 11u^2 = 1$ genügende ganze Zahlen bezeichnen.

lichen Transformationen der Form (2, 5, 7) in die Form (275, 0, — 1) unter den folgenden beiden Formeln enthalten sind:

I. $65t - 1100u,\ 4t - 65u,\ -15t + 275u,\ -t + 15u,$
II. $10t + 275u,\ -t - 10u,\ -15t - 275u,\ t + 15u.$

Formen mit der Determinante 0.

215.

Bisher haben wir Formen mit der Determinante 0 aus allen Untersuchungen ausgeschlossen; wir müssen daher, damit unsere Theorie in jeder Beziehung vollständig werde, über diese noch Einiges hinzufügen. Da allgemein bewiesen ist, dass, wenn irgend eine Form mit der Determinante D eine Form mit der Determinante D' enthält, D' ein Vielfaches von D ist, so ist sogleich klar, dass eine Form, deren Determinante gleich 0 ist, eine andere Form, als eine solche, deren Determinante ebenfalls gleich 0 ist, nicht enthalten kann. Daher bleiben nur zwei Aufgaben zu lösen, nämlich: 1. Wenn zwei Formen f, F, deren letztere die Determinante 0 hat, gegeben sind, so soll man entscheiden, ob die erstere die letztere enthält oder nicht, und in jenem Falle sämtliche Transformationen jener in diese darstellen. 2. Man soll alle Darstellungen einer gegebenen Zahl durch eine gegebene Form mit der Determinante 0 finden. Die erste Aufgabe erfordert ein anderes Verfahren, wenn die Determinante der ersteren Form f ebenfalls 0 ist, als wenn sie nicht gleich 0 ist. Dies alles werden wir jetzt auseinandersetzen.

I. Vor allem bemerken wir, dass jede Form $ax^2 + 2bxy + cy^2$, deren Determinante $b^2 - ac = 0$ ist, in der Form $m(gx + hy)^2$ dargestellt werden kann, wo g und h zu einander prime Zahlen sind und m eine ganze Zahl bezeichnet. Ist nämlich m der grösste gemeinschaftliche Teiler der Zahlen a, c und zwar mit demselben Zeichen genommen, welches diese Zahlen selbst haben (dass diese Zahlen keine entgegengesetzten Zeichen haben können, ist leicht ersichtlich), so werden $\frac{a}{m}$, $\frac{c}{m}$ ganze zu einander prime nicht negative Zahlen und ihr Product gleich $\frac{b^2}{m^2}$ d. h. ein Quadrat und sie selbst somit Quadrate sein (Artikel 21). Ist $\frac{a}{m} = g^2$, $\frac{c}{m} = h^2$, so sind auch g und h zu einander prim, ferner ist $g^2h^2 = \frac{b^2}{m^2}$ und $gh = \pm\frac{b}{m}$. Hieraus geht hervor, dass

$$m(gx \pm hy)^2 = ax^2 + 2bxy + cy^2$$

ist.

Es seien nun zwei Formen f, F, beide mit der Determinante 0, gegeben, und zwar sei:

$$f = m(gx + hy)^2, \quad F = M(GX + HY)^2,$$

so dass g zu h und G zu H prim ist. Dann behaupte ich, dass, wenn die Form f die Form F enthält, m entweder gleich M ist oder wenigstens in M aufgeht und dass der Quotient eine Quadratzahl ist, und umgekehrt, dass, wenn $\frac{M}{m}$ eine ganze Quadratzahl ist, F unter f enthalten ist. Nimmt man nämlich an, dass f durch die Substitution

$$x = \alpha X + \beta Y, \quad y = \gamma X + \delta Y$$

in F übergehe, so wird:

$$\frac{M}{m}(GX + HY)^2 = [(\alpha g + \gamma h)X + (\beta g + \delta h)Y]^2,$$

woraus leicht folgt, dass $\frac{M}{m}$ ein Quadrat ist. Setzt man dasselbe gleich e^2, so wird:

$$e(GX + HY) = \pm[(\alpha g + \gamma h)X + (\beta g + \delta h)Y], \text{ d. i.}$$
$$\pm eG = \alpha g + \gamma h, \quad \pm eH = \beta g + \delta h.$$

Wenn daher $\mathfrak{G}$, $\mathfrak{H}$ so bestimmt werden, dass $\mathfrak{G}G + \mathfrak{H}H = +1$ ist, so hat man:

$$\pm e = \mathfrak{G}(\alpha g + \gamma h) + \mathfrak{H}(\beta g + \delta h) = \text{einer ganzen Zahl.}$$

Wenn aber umgekehrt angenommen wird, dass $\frac{M}{m}$ eine ganze Quadratzahl und gleich e^2 sei, so wird die Form f die Form F enthalten. Es werden nämlich ganze Zahlen α, β, γ, δ so bestimmt werden können, dass

$$\alpha g + \gamma h = \pm eG, \quad \beta g + \delta h = \pm eH$$

ist. Denn nimmt man ganze Zahlen $\mathfrak{g}$, $\mathfrak{h}$ so an, dass $\mathfrak{g}g + \mathfrak{h}h = 1$ ist, so wird man jenen Gleichungen genügen, wenn man setzt:

$$\alpha = \pm eG\mathfrak{g} + hz, \quad \gamma = \pm eG\mathfrak{h} - gz,$$
$$\beta = \pm eH\mathfrak{g} + hz', \quad \delta = \pm eH\mathfrak{h} - gz',$$

welche ganzzahligen Werte man auch z und z' beilegen möge. Daher wird F in f enthalten sein. Zugleich erkennt man ohne Schwierigkeit, dass diese Formeln alle Werte, welche α, β, γ, δ erhalten können, d. h. alle Transformationen der Form f in F darstellen, wofern nur angenommen wird, dass z, z' unbestimmt alle ganzen Zahlen darstellen.

II. Wenn zwei Formen $f = ax^2 + 2bxy + cy^2$, deren Determinante nicht gleich 0 ist, und $F = M(GX + HY)^2$, deren Determinante gleich 0 ist, gegeben sind, so behaupte ich erstens, dass, wenn f die Form F enthält, die Zahl M durch die Form f dargestellt werden kann; zweitens, dass, wenn M durch f dargestellt werden kann, F unter f enthalten ist; drittens, dass, wenn in diesem Falle alle Darstellungen der Zahl M durch die Form f

unbestimmt durch $x = \xi$, $y = \upsilon$ dargestellt werden, alle Transformationen der Form f in F sich in der Form $G\xi$, $H\xi$, $G\upsilon$, $H\upsilon$ darstellen. Dies alles beweisen wir folgendermassen.

1. Nehmen wir an, dass f in F durch die Substitution $\alpha, \beta, \gamma, \delta$ übergehe, und bestimmen wir die Zahlen $\mathfrak{G}$, $\mathfrak{H}$ derart, dass $\mathfrak{G}G + \mathfrak{H}H = 1$ ist, so wird offenbar, wenn $x = \alpha\mathfrak{G} + \beta\mathfrak{H}$, $y = \gamma\mathfrak{G} + \delta\mathfrak{H}$ gesetzt wird, der Wert der Form f gleich M werden und daher M durch die Form f darstellbar sein.

2. Nimmt man an, dass $a\xi^2 + 2b\xi\upsilon + c\upsilon^2 = M$ sei, so geht offenbar durch die Substitution $G\xi$, $H\xi$, $G\upsilon$, $H\upsilon$ die Form f in F über. Dass aber

3. in diesem Falle die Substitution $G\xi$, $H\xi$, $G\upsilon$, $H\upsilon$ alle Transformationen der Form f in F giebt, wenn man annimmt, dass ξ, υ alle Werte von x, y darstellen, welche $f = M$ machen, erkennt man so: Ist $\alpha, \beta, \gamma, \delta$ irgend eine Transformation der Form f in F und wie vorher $\mathfrak{G}G + \mathfrak{H}H = 1$, so werden sich unter den Werten von x, y auch die folgenden befinden:

$$x = \alpha\mathfrak{G} + \beta\mathfrak{H}, \quad y = \gamma\mathfrak{G} + \delta\mathfrak{H},$$

und aus diesen erhält man die Substitution:

$$G(\alpha\mathfrak{G} + \beta\mathfrak{H}), \quad H(\alpha\mathfrak{G} + \beta H), \quad G(\gamma\mathfrak{G} + \delta\mathfrak{H}), \quad H(\gamma\mathfrak{G} + \delta\mathfrak{H}),$$

oder:

$$\alpha + \mathfrak{H}(\beta G - \alpha H), \quad \beta + \mathfrak{G}(\alpha H - \beta G)$$
$$\gamma + \mathfrak{H}(\delta G - \gamma H), \quad \delta + \mathfrak{G}(\gamma H - \delta G).$$

Da aber

$$a(\alpha X + \beta Y)^2 + 2b(\alpha X + \beta Y)(\gamma X + \delta Y) + c(\gamma X + \delta Y)^2 = M(GX + HY)^2$$

ist, so wird:

$$a(\alpha\delta - \beta\gamma)^2 = M(\delta G - \gamma H)^2$$
$$c(\beta\gamma - \alpha\delta)^2 = M(\beta G - \alpha H)^2,$$

und daher (da die Determinante der Form f mit $(\alpha\delta - \beta\gamma)^2$ multipliciert gleich der Determinante der Form F, d. h. gleich 0 und somit auch $\alpha\delta - \beta\gamma = 0$ ist):

$$\delta G - \gamma H = 0, \quad \beta G - \alpha H = 0.$$

Demnach geht jene Substitution über in $\alpha, \beta, \gamma, \delta$, woraus hervorgeht, dass die angegebene Formel alle Transformationen der Form f in F liefert.

III. Es bleibt uns noch zu zeigen übrig, wie man alle Darstellungen einer gegebenen Zahl durch eine gegebene Form mit der Determinante 0 angeben kann. Ist $m(gx + hy)^2$ die gegebene Form, so erhellt sogleich, dass jene Zahl durch m teilbar und der Quotient ein Quadrat sein muss. Wird daher die gegebene Zahl gleich me^2 gesetzt, so ist ersichtlich, dass für diejenigen Werte von x, y, für welche $m(gx + hy)^2 = me^2$ wird, auch $gx + hy$ entweder gleich $+e$ oder gleich $-e$ wird. Daher erhält man alle Darstellungen, wenn man alle Lösungen der linearen Gleichungen $gx + hy = e$ und $gx + hy = -e$ in ganzen Zahlen gefunden hat. Dass aber diese lösbar sind, ist bekannt (wenn nämlich, wie vorausgesetzt wird,

g und h zu einander prim sind). Wenn nämlich $\mathfrak{g}$, $\mathfrak{h}$ so bestimmt werden, dass $\mathfrak{g}g + \mathfrak{h}h = 1$ ist, so wird der ersteren Gleichung genügt werden, wenn man setzt: $x = \mathfrak{g}e + \mathfrak{h}z$, $y = \mathfrak{h}e - gz$, der letzteren aber, wenn man setzt: $x = -\mathfrak{g}e + hz$, $y = -\mathfrak{h}e - gz$, wo z irgend eine ganze Zahl bezeichnet. Zu gleicher Zeit aber werden diese Formeln alle ganzzahligen Werte von x, y ergeben, wenn man annimmt, dass z unbestimmt jede ganze Zahl bezeichnet.

Allgemeine Auflösung aller unbestimmten Gleichungen zweiten Grades mit zwei Unbekannten durch ganze Zahlen.

216.

Als Schluss dieser Untersuchungen fügen wir hinzu die

Aufgabe: Alle Lösungen der allgemeinen*) unbestimmten Gleichung zweiten Grades mit zwei Unbekannten

$$ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0$$

(wo a, b, c, ... beliebige gegebene ganze Zahlen sind) durch ganze Zahlen zu finden.

Auflösung. Wir führen an Stelle der Unbekannten x, y andere ein:

$$p = (b^2 - ac)x + be - cd, \quad q = (b^2 - ac)y + bd - ae,$$

welche offenbar stets ganze Zahlen sein werden, wenn x und y ganze Zahlen sind. Dadurch erhält man die Gleichung:

$$ap^2 + 2bpq + cq^2 + f(b^2 - ac)^2 + (b^2 - ac)(ae^2 - 2bde + cd^2) = 0,$$

oder, wenn wir der Kürze wegen die Zahl

$$f(b^2 - ac)^2 + (b^2 - ac)(ae^2 - 2bde + cd^2) = -M$$

setzen:

$$ap^2 + 2bpq + cq^2 = M.$$

Nun haben wir im Vorhergehenden gezeigt, wie man sämtliche Lösungen dieser Gleichung, d. h. sämtliche Darstellungen der Zahl M durch die Form (a, b, c), finden kann. Wenn aber aus den einzelnen Wertepaaren von p, q die entsprechenden Werte von x, y mit Hülfe der Gleichungen

$$x = \frac{p + cd - be}{b^2 - ac}, \quad y = \frac{q + ae - bd}{b^2 - ac}$$

bestimmt werden, so sieht man leicht, dass alle diese Werte der gegebenen Gleichung genügen, und dass es keine ganzzahligen Werte von x, y giebt,

*) Wenn eine Gleichung gegeben wäre, in welcher der zweite, vierte oder fünfte Coefficient nicht gerade wäre, würde sie durch Multiplikation mit 2 die hier vorausgesetzte Form erhalten.

welche nicht auf diese Weise erhalten würden. Wenn wir daher aus allen so entstehenden Werten von x, y die gebrochenen Werte weglassen, so werden alle gesuchten Lösungen übrig bleiben.

Hinsichtlich dieser Lösung sind folgende Bemerkungen zu machen.

1. Wenn sich entweder die Zahl M nicht durch die Form (a, b, c) darstellen lässt, oder aus keiner Darstellung sich ganzzahlige Werte von x, y ergeben, so lässt sich die Gleichung in keiner Weise durch ganze Zahlen lösen.

2. Wenn die Determinante der Form (a, b, c) d. h. die Zahl $b^2 - ac$ negativ oder positiv und quadratisch und zugleich M nicht gleich 0 ist, so wird die Anzahl der Darstellungen der Zahl M durch die Form (a, b, c) eine endliche und somit auch die Anzahl aller Lösungen der gegebenen Gleichung (wenn es deren überhaupt giebt) eine endliche sein.

3. Wenn $b^2 - ac$ eine positive nichtquadratische oder eine quadratische Zahl und gleichzeitig $M = 0$ ist, so wird die Zahl M, wenn überhaupt auf eine Weise, auf unendlich viele verschiedene Weisen durch die Form (a, b, c) dargestellt werden können; da es aber unmöglich ist, alle diese Darstellungen selbst zu finden und zu versuchen, ob sie ganzzahlige Werte von x, y liefern oder gebrochene, so ist es notwendig, eine Regel anzugeben, durch welche wir, falls etwa gar keine Darstellung ganzzahlige Werte von x, y liefert, über diesen Punkt Gewissheit erhalten können (denn wir würden, wie viele Darstellungen wir auch in diesem Falle untersucht haben würden, doch niemals ohne eine solche Regel zur Gewissheit kommen); wenn aber einige Darstellungen ganzzahlige, andere gebrochene Werte von x, y ergeben, so wird zu zeigen sein, wie man diese von jenen von vornherein allgemein unterscheiden kann.

4. Ist $b^2 - ac = 0$, so können die Werte von x, y durch die vorher angegebenen Formeln überhaupt nicht bestimmt werden; daher muss man für diesen Fall ein besonderes Verfahren ermitteln.

217.

Für den Fall, wo $b^2 - ac$ eine positive nichtquadratische Zahl ist, haben wir oben gezeigt, dass sämtliche Darstellungen der Zahl M durch die Form $ap^2 + 2bpq + cq^2$ (wenn es deren überhaupt giebt) durch eine oder mehrere solche Formeln wie

$$p = \frac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), \qquad q = \frac{1}{m}(\mathfrak{C}t + \mathfrak{D}u)$$

bestimmt werden können, wobei $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ gegebene ganze Zahlen, m den grössten gemeinschaftlichen Teiler der Zahlen a, $2b$, c, endlich t, u unbestimmt alle der Gleichung $t^2 - (b^2 - ac)\,u^2 = m^2$ genügenden ganze Zahlen bezeichnen. Da sämtliche Werte von t, u sowohl positiv wie negativ an-

genommen werden können, so können wir für jede einzelne jener Formeln vier andere substituieren:

$$p = \frac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), \quad q = \frac{1}{m}(\mathfrak{C}t + \mathfrak{D}u)$$

$$p = \frac{1}{m}(\mathfrak{A}t - \mathfrak{B}u), \quad q = \frac{1}{m}(\mathfrak{C}t - \mathfrak{D}u)$$

$$p = \frac{1}{m}(-\mathfrak{A}t + \mathfrak{B}u), \quad q = \frac{1}{m}(-\mathfrak{C}t + \mathfrak{D}u)$$

$$p = -\frac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), \quad q = -\frac{1}{m}(\mathfrak{C}t + \mathfrak{D}u),$$

so dass die Anzahl aller Formeln jetzt viermal so gross ist als vorher, t und u aber nicht mehr alle der Gleichung $t^2 - (b^2 - ac)u^2 = m^2$ genügenden Zahlen, sondern nur die positiven Zahlen dieser Art ausdrücken. Jede dieser Formen muss daher für sich betrachtet und untersucht werden, welche Werte von t, u ganzzahlige Werte von x, y liefern.

Aus den Ausdrücken

[1] $$p = \frac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), \qquad q = \frac{1}{m}(\mathfrak{C}t + \mathfrak{D}u)$$

ergeben sich folgende Werte von x, y:

$$x = \frac{\mathfrak{A}t + \mathfrak{B}u + mcd - mbe}{m(b^2 - ac)}, \quad y = \frac{\mathfrak{C}t + \mathfrak{D}u + mae - mbd}{m(b^2 - ac)}.$$

Oben haben wir aber gezeigt, dass alle (positiven) Werte von t eine rekurrente Reihe $t^0, t', t'', \ldots$ und ebenso auch die entsprechenden Werte von u eine rekurrente Reihe $u^0, u', u'', \ldots.$ bilden; dass ferner eine Zahl ρ von solcher Beschaffenheit angegeben werden kann, dass nach irgend einem gegebenen Modul

$$t^{(\rho)} \equiv t^0, \quad t^{(\rho+1)} \equiv t', \quad t^{(\rho+2)} \equiv t'', \ldots, \quad u^{(\rho)} \equiv u^0, \quad u^{(\rho+1)} \equiv u', \ldots$$

wird. Als diesen Modul nehmen wir die Zahl $m(b^2 - ac)$ und bezeichnen der Kürze wegen die Werte von x, y, welche entstehen, wenn man $t = t^0$, $u = u^0$ setzt, und denen wir den Index 0 beilegen, mit x^0, y^0; ebenso diejenigen, welche entstehen, wenn man $t = t'$, $u = u'$ setzt, mit x', y', denen wir den Index 1 beilegen, u. s. w. Dann sieht man ohne Mühe, dass, wenn $x^{(h)}$, $y^{(h)}$ ganze Zahlen sind und ρ richtig bestimmt ist, auch $x^{(h+\rho)}$, $y^{(h+\rho)}$ ebenso $x^{(h+2\rho)}$, $y^{(h+2\rho)}$ und allgemein $x^{(h+k\rho)}$, $y^{(h+k\rho)}$ ganze Zahlen sein werden, dass dagegen, wenn $x^{(h)}$ oder $y^{(h)}$ gebrochen ist, auch $x^{(h+k\rho)}$ oder $y^{(h+k\rho)}$ eine gebrochene Zahl ist. Hieraus folgert man leicht, dass, wenn die Werte von x, y, denen die Indices $0, 1, 2, \ldots, \rho - 1$ zukommen, entwickelt werden und für jeden dieser Indices weder x noch y eine ganze Zahl ist, es überhaupt keinen Index giebt, für welchen sowohl x als auch y ganze Werte annehmen, in welchem Falle aus der Formel [1] ganze Werte von x, y nicht abgeleitet werden können. Wenn es aber unter jenen Indices irgend welche giebt,

etwa μ, μ', μ'', ..., denen ganze Werte von x, y entsprechen, so werden sämtliche ganzen Werte von x, y, die sich nämlich aus der Formel [1] ableiten lassen, diejenigen sein, deren Indices unter irgend einer der Formen $\mu + k\rho$, $\mu' + k\rho$, $\mu'' + k\rho$, ... enthalten sind, wobei k unbestimmt alle ganzen positiven Zahlen, auch die Null mit eingeschlossen, bezeichnet.

Die übrigen Formeln, unter welchen die Werte von p, q enthalten sind, sind in ganz derselben Weise zu behandeln. Wenn der Fall einträte, dass aus keiner von allen diesen Formeln ganze Werte von x, y erhalten würden, so würde die gegebene Gleichung überhaupt nicht in ganzen Zahlen gelöst werden können; so oft sie aber wirklich lösbar ist, können die sämtlichen ganzzahligen Lösungen nach den im Vorstehenden angegebenen Regeln dargestellt werden.

218.

Ist $b^2 - ac$ eine Quadratzahl und $M = 0$, so sind sämtliche Werte von p, q enthalten unter zwei Formeln von der Art wie $p = \mathfrak{A}z$, $q = \mathfrak{B}z$; $p = \mathfrak{A}'z$, $q = \mathfrak{B}'z$, wo z unbestimmt jede ganze Zahl bezeichnet, $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{A}'$, $\mathfrak{B}'$ aber gegebene ganze Zahlen sind, deren erste mit der zweiten, deren dritte mit der vierten keinen gemeinschaftlichen Teiler hat (Artikel 212). Alle aus der ersten Formel entstehenden ganzzahligen Werte von x, y sind daher unter der Formel enthalten:

$$[1] \qquad x = \frac{\mathfrak{A}z + cd - be}{b^2 - ac}, \quad y = \frac{\mathfrak{B}z + ae - bd}{b^2 - ac},$$

und alle übrigen aus der zweiten Formel entspringenden unter der folgenden:

$$[2] \qquad x = \frac{\mathfrak{A}'z + cd - be}{b^2 - ac}, \quad y = \frac{\mathfrak{B}'z + ae - bd}{b^2 - ac}.$$

Da aber jede der beiden Formeln auch gebrochene Werte liefern kann (wofern nicht gerade $b^2 - ac = 1$ ist), so müssen wir diejenigen Werte von z, für welche sowohl x als auch y eine ganze Zahl wird, von den übrigen in jeder der beiden Formeln abscheiden; jedoch genügt es, nur die erste Formel zu betrachten, da für die andere genau dasselbe Verfahren anzuwenden ist.

Da $\mathfrak{A}$, $\mathfrak{B}$ prim zu einander sind, so kann man zwei Zahlen $\mathfrak{a}$, $\mathfrak{b}$ so bestimmen, dass $\mathfrak{a}\mathfrak{A} + \mathfrak{b}\mathfrak{B} = 1$ wird, Ist dies geschehen, so hat man:

$$(\mathfrak{a}x + \mathfrak{b}y)(b^2 - ac) = z + \mathfrak{a}(cd - be) + \mathfrak{b}(ae - bd),$$

woraus sogleich hervorgeht, dass alle Werte von z, welche ganze Werte von x, y hervorbringen können, notwendig der Zahl $\mathfrak{a}(be - cd) + \mathfrak{b}(bd - ae)$ nach dem Modul $b^2 - ac$ congruent oder unter der Formel $(b^2 - ac)z' + \mathfrak{a}(be - cd) + \mathfrak{b}(bd - ae)$, wo z' unbestimmt eine ganze Zahl bezeichnet, enthalten sein müssen. Hiernach erhalten wir leicht an Stelle der Formel [1] die folgende:

$$x = \mathfrak{A}z' + \mathfrak{b} \cdot \frac{\mathfrak{A}(bd - ae) - \mathfrak{B}(be - cd)}{b^2 - ac}$$

$$y = \mathfrak{B}z' - \mathfrak{a} \cdot \frac{\mathfrak{A}(bd - ae) - \mathfrak{B}(be - cd)}{b^2 - ac}$$

die offenbar entweder für alle Werte von z' oder für gar keine ganze Werte von x, y liefern wird, und zwar wird der erste Fall stattfinden, wenn $\mathfrak{A}(bd - ae)$ und $\mathfrak{B}(be - cd)$ nach dem Modul $b^2 - ac$ congruent, der zweite, wenn sie incongruent sind. — Auf genau dieselbe Weise ist die Formel [2] zu behandeln, und die ganzzahligen Lösungen (wenn sie deren giebt) sind von den andern zu unterscheiden.

219.

Ist $b^2 - ac = 0$, so kann die Form $ax^2 + 2bxy + cy^2$ in der Form $m(\alpha x + \beta y)^2$ dargestellt werden, wo m, α, β ganze Zahlen sind (Artikel 215). Setzt man $\alpha x + \beta y = z$, so geht die gegebene Gleichung in folgende über:

$$mz^2 + 2dx + 2ey + f = 0,$$

und hieraus folgt in Verbindung mit $\alpha x + \beta y = z$:

$$x = \frac{\beta mz^2 + 2ez + \beta f}{2\alpha e - 2\beta d}, \quad y = \frac{\alpha mz^2 + 2dz + \alpha f}{2\beta d - 2\alpha e}.$$

Nun ist klar, dass, wenn nicht $\alpha e = \beta d$ ist (welchen Fall wir sogleich für sich betrachten werden), die aus diesen Formeln dadurch, dass man z irgend einen Wert giebt, abgeleiteten Werte von x, y der gegebenen Gleichung genügen; es bleibt daher nur noch übrig zu zeigen, wie man diejenigen Werte von z bestimmt, aus denen sich ganzzahlige Werte von x, y ergeben.

Da $\alpha x + \beta y = z$ ist, so dürfen schlechterdings für z nur ganzzahlige Werte genommen werden; überdies ist klar, dass, wenn für irgend einen Wert von z sowohl x als y eine ganze Zahl wird, alle Werte von z, welche jenem nach dem Modul $2\alpha e - 2\beta d$ congruent sind, ebenfalls ganze Werte hervorbringen werden. Wenn daher für z alle ganzen Zahlen von 0 bis $2\alpha e - 2\beta d - 1$ (falls $\alpha e - \beta d$ positiv) oder bis $2\beta d - 2\alpha e - 1$ (wenn $\alpha e - \beta d$ negativ) incl. substituiert werden und für keinen dieser Werte x und y ganze Zahlen werden, so wird überhaupt kein Wert von z ganzzahlige Werte von x, y hervorbringen, und die gegebene Gleichung wird in ganzen Zahlen überhaupt nicht lösbar sein. Wenn aber einige von den Werten von z, z. B. ζ, ζ', ζ'', ... (die man auch durch Auflösung von Congruenzen zweiten Grades nach den Principien des vierten Abschnittes finden kann), für x, y ganzzahlige Werte liefern, so werden sämtliche Lösungen sich ergeben, wenn man $z = (2\alpha e - 2\beta d)v + \zeta$, $z = (2\alpha e - 2\beta d)v + \zeta'$, ... setzt, wo v unbestimmt alle ganzen Zahlen bezeichnet.

220.

Für den ausgeschlossenen Fall, in welchem $\alpha e = \beta d$ ist, müssen wir ein besonderes Verfahren ermitteln. Nehmen wir an, dass α, β prim zu einander sind, was bekanntlich nach Artikel 215, I erlaubt ist,

so ist $\frac{d}{\alpha} = \frac{e}{\beta}$ eine ganze Zahl (Artikel 19), die wir gleich h setzen. Dann nimmt die gegebene Gleichung folgende Form an:

$$(m\alpha x + m\beta y + h)^2 - h^2 + mf = 0$$

und kann daher offenbar rational nur gelöst werden, wenn $h^2 - mf$ eine Quadratzahl ist. Ist $h^2 - mf = k^2$, so ist klar, dass der gegebenen Gleichung die beiden folgenden äquivalent sind:

$$m\alpha x + m\beta y + h + k = 0 \quad \text{und} \quad m\alpha x + m\beta y + h - k = 0,$$

d. h. dass jede Lösung der gegebenen Gleichung auch der einen oder andern von diesen Gleichungen genügt und umgekehrt. Die erste Gleichung lässt sich offenbar in ganzen Zahlen nur dann lösen, wenn $h + k$ durch m teilbar ist; analog besitzt die zweite Gleichung nur dann eine Lösung in ganzen Zahlen, wenn $h - k$ durch m teilbar ist. Diese Bedingungen genügen aber auch zur Auflösbarkeit jeder der beiden Gleichungen (weil angenommen wird, dass α und β prim zu einander sind), und sämtliche Lösungen derselben können nach den bekannten Regeln gefunden werden.

221.

Den im Artikel 217 betrachteten Fall (welcher von allen der schwierigste ist) erläutern wir durch ein **Beispiel**. Gegeben sei die Gleichung:

$$x^2 + 8xy + y^2 + 2x - 4y + 1 = 0.$$

Aus dieser leiten wir zunächst durch Einführung anderer Unbekannten

$$p = 15x - 9, \quad q = 15y + 6$$

die Gleichung ab:

$$p^2 + 8pq + q^2 = -540.$$

Man findet aber, dass sämtliche ganzzahligen Lösungen dieser unter den folgenden vier Formeln enthalten sind:

$$\begin{aligned} p &= 6t, & q &= -24t - 90u \\ p &= 6t, & q &= -24t + 90u \\ p &= -6t, & q &= 24t - 90u \\ p &= -6t, & q &= 24t + 90u, \end{aligned}$$

wo t, u unbestimmt alle positiven ganzen Zahlen bezeichnen, welche der Gleichung $t^2 - 15u^2 = 1$ genügen und in den Formeln enthalten sind:

$$t = \frac{1}{2}\left[(4 + \sqrt{15})^n + (4 - \sqrt{15})^n\right]$$
$$u = \frac{1}{2\sqrt{15}}\left[(4 + \sqrt{15})^n - (4 - \sqrt{15})^n\right],$$

wenn n unbestimmt alle positiven ganzen Zahlen (auch die Null mit ein-

geschlossen) bezeichnet. Daher sind sämtliche Werte von x, y enthalten in den Formeln:

$$x = \tfrac{1}{5}(2t+3), \quad y = -\tfrac{1}{5}(8t+30u+2)$$
$$x = \tfrac{1}{5}(2t+3), \quad y = -\tfrac{1}{5}(8t-30u+2)$$
$$x = \tfrac{1}{5}(-2t+3), \quad y = \tfrac{1}{5}(8t-30u-2)$$
$$x = \tfrac{1}{5}(-2t+3), \quad y = \tfrac{1}{5}(8t+30u-2).$$

Wendet man aber unsere Regeln vorschriftsmässig an, so findet man, dass man, damit sich ganzzahlige Werte ergeben, in der ersten und zweiten Formel diejenigen Werte von t, u nehmen muss, welche aus geradem Exponenten n entstehen, in der dritten und vierten aber diejenigen, welche aus ungeradem n erhalten werden. — Als einfachste Lösungen erhält man: $x = 1, -1, -1$, $y = -2, 0, 12$ respective.

Übrigens mag bemerkt werden, dass die Auflösung des im vorhergehenden Artikel behandelten Problems in den meisten Fällen durch mannigfache Kunstgriffe abgekürzt werden kann, besonders hinsichtlich der Ausschliessung untauglicher d. h. Brüche enthaltender Lösungen. Doch sehen wir uns, um nicht allzu weitläufig zu werden, genötigt, dies an dieser Stelle zu übergehen.

Geschichtliche Bemerkungen.

222.

Da Vieles von dem, was wir bisher behandelt haben, auch von andern Geometern in Betracht gezogen worden ist, können wir die Verdienste dieser nicht stillschweigend übergehen. Über die Äquivalenz der Formen hat allgemeine Untersuchungen angestellt Lagrange, *Nouv. Mém. de l'Ac. de Berlin, 1773 p. 263* und *1775 p. 323 u. ff.*, wo er besonders zeigte, dass es für jede gegebene Determinante eine endliche Anzahl von Formen von solcher Beschaffenheit giebt, dass jede Form mit jener Determinante irgend einer von ihnen äquivalent ist, und dass somit alle Formen mit gegebener Determinante in Klassen geteilt werden können. Später hat Legendre mehrere elegante Eigenschaften dieser Klassifikation zum grössten Teil durch Induction entdeckt, die wir unten angeben und durch Beweise erhärten werden. Übrigens ist bisher Niemand auf die Unterscheidung der eigentlichen und uneigentlichen Aequivalenz, deren Nutzen besonders in den feineren Untersuchungen zu Tage tritt, gekommen.

Das berühmte im Artikel 216 u. ff. entwickelte Problem hat zuerst Lagrange vollständig gelöst, *Hist. de l'Ac. de Berlin, 1767 p. 165* und *1768 p. 181 u. ff.* Es findet sich auch eine (minder vollständige) Lösung in den schon öfter erwähnten Supplementen zu Euler's Algebra. Schon vorher hatte Euler denselben Gegenstand in Angriff genommen, *Comm. Petr. T. VI p. 175; Comm. Nov. T. IX, p. 3;* ebendaselbst *T. XVIII, p. 185 u. ff.*; doch

beschränkte er seine Untersuchung immer darauf, aus irgend einer Lösung, die er als bereits bekannt annimmt, andere abzuleiten, und überdies vermögen seine Methoden nur in wenigen Fällen sämtliche Lösungen zu liefern (vgl. Lagrange, *Hist. de l'Ac. de Berlin, 1767, p. 237*). Da die letzte dieser drei Abhandlungen jüngeren Datums ist als die Lagrange'sche, welche die Aufgabe in ihrer ganzen Allgemeinheit erfasst und in dieser Beziehung nichts zu wünschen übrig lässt, so scheint Euler zu jener Zeit (der achtzehnte Band der Commentare gehört zum Jahre 1773 und wurde 1774 veröffentlicht) jene Lösung noch nicht gekannt zu haben. Übrigens baut sich unsere Lösung (sowie Alles andere, was wir in diesem Abschnitte bisher angegeben haben) auf ganz verschiedenen Prinzipien auf.

Was von andern, Diophant, Fermat u. s. w., hierher Gehöriges überliefert worden ist, betrifft nur die speciellsten Fälle; wir entheben uns daher der Mühe, da wir das, was besonders erwähnenswert erschien, schon oben angeführt haben, alles einzeln aufzuzählen.

Was wir bisher von den Formen zweiten Grades auseinandergesetzt haben, ist nur als der erste Anfang dieser Lehre zu betrachten; während wir diese Untersuchung eifriger verfolgten, eröffnete sich uns ein sehr weites Feld, von dem wir das, was besonders der Aufmerksamkeit wert erscheint, im Folgenden darlegen werden. Denn dieser Gegenstand ist so fruchtbar, dass wir vieles andere, was uns schon jetzt zu finden gelungen ist, der Kürze halber mit Stillschweigen übergehen müssen; weit mehr aber liegt ohne Zweifel noch verborgen und harrt erneuter Anstrengungen. Übrigens wollen wir gleich am Beginne dieser Untersuchungen bemerken, dass Formen mit der Determinante 0 davon ausgeschlossen sind, falls nicht das Gegenteil ausdrücklich hervorgehoben wird.

Weitere Untersuchungen über die Formen.

Einteilung der Formen mit gegebener Determinante in Klassen.

223.

Schon oben (Artikel 175, 195, 211) haben wir gezeigt, dass, wenn irgend eine ganze (sei es positive, sei es negative) Zahl D gegeben ist, eine endliche Anzahl von Formen F, F', F'', ... mit der Determinante D von der Beschaffenheit angegeben werden kann, dass jede beliebige Form mit der Determinante D irgend einer von jenen und nur einer einzigen eigentlich äquivalent ist. Somit können sämtliche Formen mit der Determinante D (deren Anzahl unendlich gross ist) nach jenen Formen in

Klassen geteilt werden, indem man nämlich aus der Gesamtheit aller Formen, welche der Form F eigentlich äquivalent sind, die erste Klasse, aus den Formen, welche der Form F' eigentlich äquivalent sind, die zweite Klasse, u. s. w. bildet.

Aus den einzelnen Klassen der Formen mit der gegebenen Determinante D kann irgend eine Form ausgewählt und gleichsam als **repräsentierende** Form (Repräsentant) der ganzen Klasse betrachtet werden. An sich ist es zwar vollständig gleichgültig, welche Form man aus jeder Klasse nimmt, indessen wird stets diejenige den Vorzug verdienen, welche die andern an Einfachheit zu übertreffen scheint. Die Einfachheit irgend einer Form (a, b, c) wird offenbar nach der Grösse der Zahlen a, b, c zu beurteilen sein, und mit Recht wird die Form (a', b', c') minder einfach genannt werden als (a, b, c), wenn $a' > a, b' > b, c' > c$ ist. Hierdurch ist aber die Sache noch nicht völlig bestimmt, und bleibt es z. B. unserm Belieben überlassen, welche der beiden Formen $(17, 0, -45)$, $(5, 0, -153)$ wir für die einfachere halten wollen. Meistens jedoch wird es zweckmässig sein, die folgende Regel zu beobachten.

I. Wenn die Determinante D negativ ist, so nehme man die reducierten Formen in den einzelnen Klassen als repräsentierende Formen; wo sich aber in derselben Klasse zwei reducierte Formen (welche dann entgegengesetzt sind, Artikel 172) vorfinden, nehme man diejenige, deren mittleres Glied positiv ist.

II. Wenn die Determinante D eine positive nichtquadratische Zahl ist, entwickle man die Periode irgend einer in der gegebenen Klasse enthaltenen reducierten Form, in welcher entweder zwei ambige Formen vorkommen werden oder gar keine (Artikel 187).

1. Im ersteren Falle seien (A, B, C), (A', B', C') die ambigen Formen; ferner seien die kleinsten Reste der Zahlen B, B' nach den Moduln A, A' bezüglich M, M' (welche positiv genommen werden können, wenn sie nicht gleich Null sind) und schliesslich $\frac{D-M^2}{A} = N$, $\frac{D-M'^2}{A'} = N'$. Ist dies geschehen, so nehme man von den Formen $(A, M, -N)$, $(A', M', -N')$ diejenige, welche am einfachsten zu sein scheint, als repräsentierende Form. Bei der Entscheidung hierüber gebe man derjenigen Form, deren mittleres Glied gleich Null ist, den Vorzug; wenn aber das mittlere Glied entweder in jeder von beiden Formen oder in keiner gleich 0 ist, so ist diejenige, welche das kleinere erste Glied hat, der andern vorzuziehen, und wenn die ersten Glieder an Grösse gleich, in ihren Vorzeichen aber verschieden sind, so ist dem positiven Zeichen vor dem negativen der Vorzug zu geben.

2. Wenn es aber in der ganzen Periode keine ambige Form giebt, so wähle man von sämtlichen Formen der Periode diejenige, welche ohne Rücksicht auf das Vorzeichen das kleinste erste Glied hat, so zwar, dass, wenn in derselben Periode zwei Formen vorkommen, in deren einer dasselbe

erste Glied mit positivem, in deren anderer mit negativem Vorzeichen behaftet ist, dem ersteren vor dem letzteren der Vorzug gegeben wird. Ist (A, B, C) diese Form und leitet man aus ihr in ebenderselben Weise wie im vorigen Falle eine andere Form $(A, M, -N)$ her (indem man nämlich für M den absolut kleinsten Rest von B nach dem Modul A nimmt und $N = \frac{D - M^2}{A}$ setzt), so nehme man diese schliesslich als Repräsentanten.

Wenn es aber vorkäme, dass dasselbe kleinste erste Glied A mehreren Formen der Periode gemeinsam wäre, so sind alle diese Formen in der vorgeschriebenen Weise zu behandeln und von den entstehenden Formen diejenige, deren mittleres Glied möglichst klein wird, als repräsentierende Form zu nehmen.

So hat man z. B. für $D = 305$ unter andern folgende Periode: $(17, 4, -17)$, $(-17, 13, 8)$, $(8, 11, -23)$, $(-23, 12, 7)$, $(7, 16, -7)$, $(-7, 12, 23)$, $(23, 11, -8)$, $(-8, 13, 17)$, aus der man zunächst die Form $(7, 16, -7)$ auswählt; aus dieser leitet man sodann die repräsentierende Form $(7, 2, -43)$ her.

III. Ist die Determinante eine positive Quadratzahl und gleich k^2, so ermittle man die in der gegebenen Klasse enthaltene reducierte Form $(A, k, 0)$ und nehme diese, falls $A \leqq k$ ist, als repräsentierende Form; ist aber $A > k$, so nehme man an deren Stelle die Form $(A - 2k, k, 0)$, deren erstes Glied negativ, aber kleiner als k ist.

Beispiel. Auf diese Weise zerfallen sämtliche Formen mit der Determinante -235 in sechzehn Klassen, deren Repräsentanten sind: $(1, 0, 235)$, $(2, 1, 118)$, $(4, 1, 59)$, $(4, -1, 59)$, $(5, 0, 47)$, $(10, 5, 26)$, $(13, 5, 20)$, $(13, -5, 20)$ und noch acht andere, die sich von den vorstehenden nur durch die Vorzeichen der äusseren Glieder unterscheiden, nämlich $(-1, 0, -235)$, $(-2, 1, -118)$, ...

Sämtliche Formen mit der Determinante 79 zerfallen in sechs Klassen, deren Repräsentanten sind: $(1, 0, -79)$, $(3, 1, -26)$, $(3, -1, -26)$, $(-1, 0, 79)$, $(-3, 1, 26)$, $(-3, -1, 26)$.

224.

Durch diese Klassifikation werden daher die Formen, welche eigentlich äquivalent sind, von den übrigen ganz und gar abgesondert. Zwei Formen mit derselben Determinante sind äquivalent, wenn sie derselben Klasse angehören; jede Zahl, welche durch die eine darstellbar ist, lässt sich auch durch die andere darstellen, und wenn irgend eine Zahl M durch die erste Form in der Weise dargestellt werden kann, dass die Unbestimmten zu einander prime Werte haben, so wird dieselbe Zahl durch die andere Form in derselben Weise dargestellt werden können und zwar so, dass beide Darstellungen zu demselben Werte des Ausdrucks $\sqrt{D} \pmod{M}$ gehören. Wenn aber zwei Formen zu verschiedenen Klassen gehören, so sind sie

nicht eigentlich äquivalent; von der Darstellbarkeit irgend einer gegebenen Zahl durch die eine Form lässt sich nicht auf die Darstellbarkeit derselben Zahl durch die andere Form schliessen; im Gegenteil, wenn die Zahl M durch die eine so dargestellt werden kann, dass die Werte der Unbestimmten zu einander prim sind, so sind wir sofort sicher, dass es keine ähnliche Darstellung derselben Zahl durch die andere Form giebt, welche zu demselben Werte des Ausdrucks $\sqrt{D}\,(\text{mod.}\, M)$ gehört (Vgl. Artikel 167, 168).

Dagegen ist es jedenfalls möglich, dass zwei Formen F, F' aus verschiedenen Klassen K, K' uneigentlich äquivalent sind, in welchem Falle jede Form aus der einen Klasse jeder Form aus der andern uneigentlich äquivalent sein wird; jede Form aus K hat eine ihr entgegengesetzte in K' und die Klassen K und K' selbst sollen **entgegengesetzt** heissen. So ist in dem ersten Beispiel des vorigen Artikels die dritte Klasse der Formen mit der Determinante — 235 der vierten, die siebente der achten entgegengesetzt; im zweiten Beispiel ist die zweite Klasse der dritten, die fünfte der sechsten entgegengesetzt. Sind daher irgend zwei Formen aus entgegengesetzten Klassen gegeben, so wird jede Zahl M, welche sich durch die eine darstellen lässt, auch durch die andere dargestellt werden können, und zwar wird dies, wenn es in der einen durch zu einander prime Werte geschieht, in der andern in gleicher Weise möglich sein, so zwar, dass diese beiden Darstellungen zu entgegengesetzten Werten des Ausdrucks $\sqrt{D}\,(\text{mod.}\, M)$ gehören. — Übrigens sind die oben angegebenen Regeln für die Auswahl der repräsentierenden Formen derartig beschaffen, dass entgegengesetzte Klassen stets entgegengesetzte repräsentierende Formen erhalten.

Schliesslich giebt es auch Klassen, die sich **selbst entgegengesetzt** sind. Wenn nämlich irgend eine Form zugleich mit der zu ihr entgegengesetzten in derselben Klasse enthalten ist, so erkennt man leicht, dass alle Formen dieser Klasse einander sowohl eigentlich als uneigentlich äquivalent sind, und zu jeder Form die ihr entgegengesetzte vorkommt. Dieser Art wird jede Klasse sein, in welcher eine ambige Form enthalten ist, und umgekehrt wird in jeder sich selbst entgegengesetzten Klasse notwendig eine ambige Form vorkommen (Art. 163, 165), weshalb die Klasse eine **ambige Klasse** genannt werden wird. So hat man unter den Klassen der Formen mit der Determinante — 235 acht ambige Klassen, deren Repräsentanten sind: (1, 0, 235), (2, 1, 118), (5, 0, 47), (10, 5, 26), (— 1, 0, — 235), (— 2, 1, — 118), (— 5, 0, — 47), (— 10, 5, — 26); unter den Klassen der Formen mit der Determinante 79 zwei ambige, deren Repräsentanten sind (1, 0, — 79), (— 1, 0, 79). — Wenn übrigens die repräsentierenden Formen nach unsern Regeln bestimmt sind, so kann man die ambigen Klassen ohne Schwierigkeiten erkennen. Für eine positive nichtquadratische Determinante wird nämlich eine ambige Klasse sicher eine ambige repräsentierende Form erhalten (Artikel 194); für eine negative Determinante wird die repräsentierende Form einer ambigen Klasse entweder selbst ambig oder derartig sein,

dass ihre äusseren Glieder gleich sind (Artikel 172); für eine positive quadratische Determinante endlich erkennt man nach Artikel 210 leicht, ob die repräsentierende Form sich selbst uneigentlich äquivalent und somit die von ihr repräsentierte Klasse ambig ist.

225.

Schon oben (in Artikel 175) haben wir gezeigt, dass in der Form (a, b, c) **mit negativer Determinante** die äusseren Glieder sowohl unter sich als mit den äusseren Gliedern jeder andern ihr äquivalenten Form dieselben Vorzeichen haben. Wenn a, c positiv sind, so werden wir die Form (a, b, c) eine **positive Form** nennen, und ebenso soll die ganze Klasse, in welcher (a, b, c) enthalten ist und welche nur aus positiven Formen bestehen wird, eine **positive Klasse** heissen. Andererseits wird (a, b, c) eine **negative Form** und in einer **negativen Klasse** enthalten sein, wenn a, c negativ sind. Durch eine positive Form lassen sich keine negativen, durch eine negative Form keine positiven Zahlen darstellen. Ist die Form (a, b, c) der Repräsentant irgend einer positiven Klasse, so ist die Form $(-a, b, -c)$ der Repräsentant einer negativen, woraus folgt, dass die Anzahl der positiven Klassen der Anzahl der negativen gleich ist, und dass, sobald jene bestimmt sind, auch diese gegeben sind. Daher braucht man bei den Untersuchungen über Formen mit negativer Determinante meistenteils nur positive Klassen zu betrachten, da sich deren Eigenschaften leicht auf die negativen Klassen übertragen.

Übrigens gilt diese Unterscheidung einzig und allein bei Formen mit negativer Determinante; durch Formen mit positiver Determinante lassen sich ohne Unterschied positive und negative Zahlen darstellen, ja nicht selten gehören sogar zwei Formen wie (a, b, c), $(-a, b, -c)$ in diesem Falle zu einer und derselben Klasse.

Einteilung der Klassen in Ordnungen.

226.

Irgend eine Form (a, b, c) nennen wir eine **primitive (ursprüngliche) Form,** wenn die Zahlen a, b, c keinen gemeinschaftlichen Teiler haben; sonst wird sie eine **derivierte** oder **abgeleitete Form** genannt, und zwar ist, wenn man den grössten gemeinschaftlichen Teiler der Zahlen a, b, c gleich m setzt, die Form (a, b, c) aus der ursprünglichen Form $\left(\frac{a}{m}, \frac{b}{m}, \frac{c}{m}\right)$ abgeleitet. Aus dieser Definition geht sogleich hervor, dass alle Formen, deren Determinante durch keine Quadratzahl (ausser 1) teilbar ist, notwendig ursprüngliche Formen sind. Ferner folgt aus Artikel 161, dass, wenn in irgend einer gegebenen Klasse von Formen mit der Determinante D

eine primitive Form vorkommt, sämtliche Formen dieser Klasse ursprüngliche sein werden, in welchem Falle die Klasse selbst eine **ursprüngliche** oder **primitive Klasse** genannt werden soll. Ferner ist klar, dass, wenn irgend eine Form F mit der Determinante D aus einer primitiven Form f mit der Determinante $\frac{D}{m^2}$ abgeleitet ist und die Klassen, in denen die Formen F, f respective enthalten sind, K, k sind, alle Formen der Klasse K aus der primitiven Klasse k abgeleitet sein werden; in diesem Falle werden wir daher die Klasse K selbst aus der primitiven Klasse k abgeleitet nennen.

Wenn (a, b, c) eine primitive Form ist, aber nicht a, c gleichzeitig gerade sind (d. h. wenn entweder jede der beiden oder wenigstens eine ungerade ist), so sieht man leicht, dass nicht nur $a, b, c,$ sondern auch $a, 2b, c$ einen gemeinschaftlichen Teiler nicht haben können, in welchem Falle die Form (a, b, c) eine **eigentlich primitive** oder einfach eine **eigentliche Form** genannt wird. Ist aber (a, b, c) eine primitive Form und sind die Zahlen a, c beide gerade, so werden offenbar die Zahlen a, $2b$, c den gemeinschaftlichen Teiler 2 haben (der zugleich der grösste sein wird), und soll dann (a, b, c) eine **uneigentlich primitive** oder einfach eine **uneigentliche Form** heissen.*) In diesem Falle ist b notwendig ungerade (denn sonst würde (a, b, c) keine primitive Form sein); daher ist $b^2 \equiv 1$ (mod. 4) und somit, da ac durch 4 teilbar ist, die Determinante $b^2 - ac \equiv 1$ (mod. 4). Uneigentliche Formen giebt es daher nur für eine Determinante von der Form $4n+1$, falls sie positiv, oder von der Form $-(4n+3)$, falls sie negativ ist. — Aus Artikel 161 aber ist ersichtlich, dass, wenn sich in irgend einer gegebenen Klasse eine eigentlich primitive Form findet, alle Formen dieser Klasse eigentlich primitiv sind, dass dagegen eine Klasse, welche eine uneigentlich primitive Form enthält, aus lauter uneigentlich primitiven Formen besteht. Daher wird die Klasse selbst im ersten Falle eine **eigentlich primitive Klasse** oder einfach eine **eigentliche Klasse,** im letzten Falle eine **uneigentlich primitive Klasse** oder eine **uneigentliche Klasse** genannt. So sind z. B. unter den positiven Klassen der Formen mit der Determinante —235 sechs eigentliche Klassen, nämlich diejenigen, deren Repräsentanten sind: (1, 0, 235), (4, 1, 59), (4, —1, 59), (5, 0, 47), (13, 5, 20), (13, —5, 20), und ebenso viele giebt es unter den negativen Klassen. Zwei aber sind in beiden uneigentliche Klassen. — Die Klassen der Formen mit der Determinante 79 (als einer Zahl von der Form $4n+3$) sind sämtlich eigentliche Klassen.

---

*) Wir haben diese Ausdrücke „eigentlich" und „uneigentlich" hier deshalb gewählt, weil keine passenderen zur Hand waren; wir merken dies an, damit nicht Jemand zwischen dieser Bezeichnung und der von Artikel 157 ab gebrauchten einen verborgenen Zusammenhang suche, der nicht existiert. Übrigens ist eine Zweideutigkeit hieraus sicher nicht zu befürchten.

Wenn die Form (a, b, c) abgeleitet ist und zwar aus der primitiven Form $\left(\frac{a}{m}, \frac{b}{m}, \frac{c}{m}\right)$, so kann diese entweder eigentlich oder uneigentlich primitiv sein. In dem ersten Falle ist m auch grösster gemeinschaftlicher Teiler der Zahlen a, $2b$, c; im letzteren Falle wird der grösste gemeinschaftliche Teiler dieser Zahlen gleich $2m$ sein. Hierdurch wird die Unterscheidung zwischen einer aus einer eigentlich primitiven Form abgeleiteten Form und einer aus einer uneigentlich primitiven Form abgeleiteten Form und ebenso (da sich nach Artikel 161 alle Formen derselben Klasse in dieser Beziehung gleich verhalten) zwischen einer aus einer eigentlich primitiven Klasse abgeleiteten Klasse und einer aus einer uneigentlich primitiven Klasse abgeleiteten Klasse verständlich.

Durch diese Unterscheidungen haben wir das erste Fundament erlangt, auf welchem wir die Einteilung aller Klassen der Formen mit gegebener Determinante in verschiedene **Ordnungen** aufbauen können. Zwei Klassen, deren Repräsentanten die Formen (a, b, c), (a', b', c') sind, rechnen wir zu derselben Ordnung, wenn sowohl die Zahlen a, b, c denselben grössten gemeinschaftlichen Teiler haben wie a', b', c', als auch die Zahlen a, $2b$, c denselben grössten gemeinschaftlichen Teiler wie a', $2b'$, c'. Wenn aber die eine oder die andere oder auch jede der beiden Bedingungen nicht stattfindet, so rechnen wir die Klassen zu verschiedenen Ordnungen. Hieraus geht sogleich hervor, dass alle eigentlich primitiven Klassen eine Ordnung, alle uneigentlich primitiven Klassen eine andere Ordnung bilden. Ist m^2 eine Quadratzahl, welche in der Determinante D aufgeht, so werden die aus den eigentlich primitiven Klassen mit der Determinante $\frac{D}{m^2}$ abgeleiteten Klassen eine besondere Ordnung, die aus den uneigentlich primitiven Klassen mit der Determinante $\frac{D}{m^2}$ abgeleiteten eine andere Ordnung bilden u. s. w. Wenn zufällig D durch keine Quadratzahl (ausser 1) teilbar ist, so wird es Ordnungen von abgeleiteten Klassen nicht geben, und somit wird es entweder nur eine Ordnung (wenn $D \equiv 2$ oder 3 nach dem Modul 4 ist), nämlich die Ordnung der eigentlich primitiven Klassen, oder zwei Ordnungen (wenn $D \equiv 1 \pmod{4}$) geben, nämlich die Ordnung der eigentlich primitiven und die Ordnung der uneigentlich primitiven Klassen. Nach den Prinzipien der Combinationslehre begründet man ohne Schwierigkeit die folgende **allgemeine Regel:** Wenn man $D = D' \cdot 2^{2\mu} a^{2\alpha} b^{2\beta} c^{2\gamma} \ldots$ setzt, so dass D' keinen quadratischen Factor enthält und $a, b, c, \ldots$ von einander verschiedene ungerade Primzahlen sind (auf diese Form lässt sich jede Zahl bringen, wenn man $\mu = 0$, wenn D nicht durch 4 teilbar ist, und $\alpha, \beta, \gamma, \ldots$ sämtlich gleich 0 setzt oder, was auf dasselbe hinauskommt, wenn man die Factoren $a^{2\alpha}, b^{2\beta}, c^{2\gamma}, \ldots$ weglässt, falls D durch keine ungerade Quadratzahl teilbar ist), so hat man

entweder

$(\mu+1)(\alpha+1)(\beta+1)(\gamma+1)\ldots$ Ordnungen, falls nämlich $D' \equiv 2$ oder $3 \pmod{4}$ ist,

oder

$(\mu+2)(\alpha+1)(\beta+1)(\gamma+1)\ldots$ Ordnungen, falls nämlich $D' \equiv 1 \pmod{4}$ ist.

Den Beweis dieser Regel unterdrücken wir jedoch, da er weder schwierig noch hier allzu notwendig ist.

1. Beispiel. Für $D = 45 = 5 \cdot 3^2$ hat man sechs Klassen, deren Repräsentanten sind: $(1, 0, -45)$, $(-1, 0, 45)$, $(2, 1, -22)$, $(-2, 1, 22)$, $(3, 0, -15)$, $(6, 3, -6)$. Diese zerfallen in vier Ordnungen; die erste Ordnung wird nämlich die beiden eigentlichen Klassen umfassen, deren Repräsentanten $(1, 0, -45)$ und $(-1, 0, 45)$ sind; die zweite Ordnung wird die beiden uneigentlichen Klassen, deren Repräsentanten $(2, 1, -22)$ und $(-2, 1, 22)$ sind, enthalten; die dritte Ordnung enthält nur die eine aus der eigentlichen Klasse mit der Determinante 5 abgeleitete Klasse, deren Repräsentant $(3, 0, -15)$ ist, und die vierte Ordnung endlich besteht aus der einen aus der uneigentlichen Klasse mit der Determinante 5 abgeleiteten Klasse, deren Repräsentant $(6, 3, -6)$ ist.

2. Beispiel. Die positiven Klassen mit der Determinante $-99 = -11 \cdot 3^2$ zerfallen in vier Ordnungen: Die erste Ordnung umfasst folgende eigentlich primitive Klassen*): $(1, 0, 99)$, $(4, 1, 25)$, $(4, -1, 25)$, $(5, 1, 20)$, $(5, -1, 20)$, $(9, 0, 11)$; die zweite Ordnung enthält die uneigentlichen Klassen $(2, 1, 50)$, $(10, 1, 10)$; die dritte Ordnung die aus den eigentlichen Klassen mit der Determinante -11 abgeleiteten Klassen $(3, 0, 33)$, $(9, 3, 12)$, $(9, -3, 12)$; die vierte Ordnung eine einzige aus der uneigentlichen Klasse mit der Determinante -11 abgeleitete Klasse $(6, 3, 18)$. — Die negativen Klassen dieser Determinante lassen sich in genau derselben Weise in Ordnungen verteilen.

Wir bemerken, dass *entgegengesetzte Klassen stets zu derselben Ordnung gehören*, ein Satz, dessen Grund ohne Schwierigkeit ersichtlich ist.

227.

Von diesen verschiedenen Ordnungen verdient *besonders die Ordnung der eigentlich primitiven Klassen die grösste Beachtung.* Denn die einzelnen abgeleiteten Klassen entstehen aus gewissen primitiven Klassen (mit kleinerer Determinante), aus deren Betrachtung das auf jene Bezügliche häufig von selbst sich ergiebt. Unten werden wir aber zeigen, dass jede uneigentlich primitive Klasse entweder einer einzigen eigentlich primitiven Klasse oder dreien (mit derselben Determinante) gewissermassen associiert ist. Ferner kann man bei negativen Determinanten die negativen Klassen bei Seite lassen, da den einzelnen derselben stets gewisse positive Klassen

---

*) Indem man der Kürze wegen die Repräsentanten für die Klassen selbst, die sie repräsentieren, anwendet.

entsprechen. Um nun die Natur der eigentlich primitiven Klassen tiefer zu durchdringen, werden wir vor Allem einen gewissen wesentlichen Unterschied darlegen, nach welchem die ganze Ordnung der eigentlichen Klassen in mehrere Geschlechter geteilt werden kann. Da wir diesen sehr wichtigen Gegenstand bisher noch nicht berührt haben, müssen wir die Sache ganz von vorn anfangen.

Teilung der Ordnungen in Geschlechter.

228.

Satz. Durch irgend eine eigentlich primitive Form F lassen sich unendlich viele Zahlen darstellen, welche durch irgend eine gegebene Primzahl p nicht teilbar sind.

Beweis. Wenn die Form $F = ax^2 + 2bxy + cy^2$ ist, so kann offenbar p nicht in allen drei Zahlen a, $2b$, c gleichzeitig aufgehen. Wenn nun a durch p nicht teilbar ist, so ist klar, dass, wenn für x irgend eine durch p nicht teilbare, für y aber eine durch p teilbare Zahl genommen wird, der Wert der Form F nicht durch p teilbar ist; ist aber c durch p nicht teilbar, so erreicht man dasselbe, wenn man x einen durch p teilbaren und y einen durch p nicht teilbaren Wert beilegt; sind endlich a und c durch p teilbar, also $2b$ nicht durch p teilbar, so wird die Form F einen durch p nicht teilbaren Wert annehmen, wenn man sowohl x als y durch p nicht teilbare Werte beilegt.

Offenbar wird der Satz auch für uneigentlich primitive Formen gelten, wofern nur nicht $p = 2$ ist.

Da mehrere derartige Bedingungen zu gleicher Zeit bestehen können, dass nämlich dieselbe Zahl durch gewisse gegebene Primzahlen teilbar, durch andere nicht teilbar sein soll (vgl. Artikel 32), so sieht man leicht, dass die Zahlen x, y auf unendlich viele Arten derart bestimmt werden können, dass die primitive Form $ax^2 + 2bxy + cy^2$ einen Wert erhält, der durch beliebig viele gegebene Primzahlen nicht teilbar ist, von denen einzig und allein die Zahl 2 auszuschliessen ist, wenn die Form uneigentlich primitiv ist. Hieraus geht hervor, dass der Satz allgemeiner folgendermassen ausgesprochen werden kann: Durch eine beliebige primitive Form können unendlich viele Zahlen dargestellt werden, welche zu irgend einer gegebenen (ungeraden Zahl, wenn die Form uneigentlich primitiv ist) Zahl prim sind.

229.

Satz. Ist F eine primitive Form mit der Determinante D und p eine in D aufgehende Primzahl, so stimmen die durch p nicht teilbaren Zahlen, welche durch die Form F dargestellt werden können, darin überein, dass sie entweder sämtlich quadratische Reste oder sämtlich quadratische Nichtreste von p sind.

Beweis. Ist $F = (a, b, c)$ und sind ferner m, m' irgend zwei durch p nicht teilbare Zahlen, welche sich durch die Form F darstellen lassen, nämlich:

$$m = ag^2 + 2bgh + ch^2, \quad m' = ag'^2 + 2bg'h' + ch'^2,$$

so ist:

$$mm' = [agg' + b(gh' + hg') + chh']^2 - D(gh' - hg')^2;$$

mithin ist mm' einem Quadrate nach dem Modul D und daher auch nach dem Modul p congruent, d. h. mm' ist quadratischer Rest von p. Hieraus folgt, dass entweder jede der beiden Zahlen m, m' quadratischer Rest oder jede quadratischer Nichtrest von p ist.

Auf ähnliche Weise beweist man, dass, wenn die Determinante D durch 4 teilbar ist, die durch F darstellbaren ungeraden Zahlen entweder sämtlich $\equiv 1$ oder sämtlich $\equiv 3 \pmod{4}$ sind. Denn in diesem Falle ist das Product aus zwei solchen Zahlen stets quadratischer Rest von 4 und daher $\equiv 1 \pmod{4}$; daher ist entweder jede der beiden $\equiv 1$ oder jede der beiden $\equiv 3$.

Wenn endlich D durch 8 teilbar ist, so ist das Product aus zwei beliebigen ungeraden Zahlen, welche durch F dargestellt werden können, quadratischer Rest von 8 und somit $\equiv 1 \pmod{8}$. Daher sind in diesem Falle die durch F darstellbaren ungeraden Zahlen entweder sämtlich $\equiv 1$ oder sämtlich $\equiv 3$ oder sämtlich $\equiv 5$ oder sämtlich $\equiv 7 \pmod{8}$.

So werden z. B., da die Zahl 10, welche Nichtrest von 7 ist, durch die Form (10, 3, 17) dargestellt werden kann, alle durch 7 nicht teilbaren Zahlen, welche sich durch jene Form darstellen lassen, Nichtreste von 7 sein. — Da -3 durch die Form $(-3, 1, 49)$ darstellbar und $\equiv 1 \pmod{4}$ ist, so werden sich alle durch diese Form darstellbaren ungeraden Zahlen in derselben Weise verhalten.

Übrigens würden wir, wenn es zum gegenwärtigen Zwecke notwendig wäre, leicht beweisen können, dass die durch F darstellbaren Zahlen zu keiner in D nicht aufgehenden Primzahl in einer derartigen festen Beziehung stehen, dass vielmehr ohne Unterschied sowohl Reste wie Nichtreste einer jeden in D nicht aufgehenden Primzahl durch die Form F dargestellt werden können. Dagegen findet hinsichtlich der Zahlen 4 und 8 etwas Analoges auch in andern Fällen statt, was wir nicht übergehen dürfen.

I. Wenn die Determinante D der primitiven Form F congruent $3 \pmod{4}$ ist, so werden die durch die Form F darstellbaren ungeraden Zahlen entweder sämtlich $\equiv 1$ oder sämtlich $\equiv 3 \pmod{4}$ sein. Sind nämlich m, m' zwei durch die Form F darstellbare Zahlen, so lässt sich das Product mm' in derselben Weise wie oben auf die Form $p^2 - Dq^2$ bringen. Wenn daher jede der beiden Zahlen m, m' ungerade ist, so muss notwendig die eine der beiden Zahlen p, q gerade, die andern ungerade und daher von den beiden Quadraten p^2, q^2 das eine $\equiv 0$, das andere $\equiv 1 \pmod{4}$ sein. Hieraus folgt leicht, dass sicher $p^2 - Dq^2 \equiv 1 \pmod{4}$ ist und daher die Zahlen m, m' entweder beide $\equiv 1$ oder beide $\equiv 3 \pmod{4}$

sind. So lassen sich z. B. durch die Form (10, 3, 17) andere ungerade Zahlen, als solche von der Form $4n + 1$, nicht darstellen.

II. Wenn die Determinante D der primitiven Form F congruent 2 (mod. 8) ist, so werden die durch F darstellbaren ungeraden Zahlen entweder sämtlich teils $\equiv 1$, teils $\equiv 7$, oder sämtlich teils $\equiv 3$, teils $\equiv 5$ (mod. 8) sein. Denn es seien m, m' zwei durch F darstellbare ungerade Zahlen, deren Product mm' sich somit auf die Form $p^2 - Dq^2$ bringen lässt. Wenn daher beide Zahlen m, m' ungerade sind, so muss notwendig p ungerade (weil D gerade ist) und daher $p^2 \equiv 1$ (mod. 8) sein; q^2 aber ist entweder $\equiv 0$ oder $\equiv 1$ oder $\equiv 4$ und somit Dq^2 entweder $\equiv 0$ oder $\equiv 2$. Hiernach wird $mm' = p^2 - Dq^2$ entweder $\equiv 1$ oder $\equiv 7$ (mod. 8). Wenn also m entweder $\equiv 1$ oder $\equiv 7$ ist, wird auch m' entweder $\equiv 1$ oder $\equiv 7$ sein, und ist m entweder $\equiv 3$ oder $\equiv 5$, so wird auch m' entweder $\equiv 3$ oder $\equiv 5$ sein. So sind z. B. alle durch die Form (3, 1, 5) darstellbaren ungeraden Zahlen entweder $\equiv 3$ oder $\equiv 5$ (mod. 8), und keine Zahl von der Form $8n + 1$ oder $8n + 7$ lässt sich durch jene Form darstellen.

III. Wenn die Determinante D der primitiven Form F congruent 6 (mod. 8) ist, so lassen sich durch diese Form ungerade Zahlen entweder nur von solcher Art, welche $\equiv 1$ und $\equiv 3$ (mod. 8) oder nur von solcher Art, welche $\equiv 5$ und $\equiv 7$ (mod. 8) sind, darstellen. Den Beweis, der dem vorigen (in II) vollkommen analog ist, wird jeder ohne Mühe entwickeln können. — So können z. B. durch die Form (5, 1, 7) nur solche ungerade Zahlen dargestellt werden, welche entweder $\equiv 5$ oder $\equiv 7$ (mod. 8) sind.

230.

Demnach werden alle Zahlen, welche durch eine gegebene primitive Form F mit der Determinante D dargestellt werden können, zu den einzelnen Primteilern von D (durch die sie nämlich nicht selbst teilbar sind) eine ganz bestimmte Beziehung haben; die ungeraden Zahlen aber, welche sich durch F darstellen lassen, werden in gewissen Fällen auch zu den Zahlen 4 und 8 eine feste Beziehung haben, nämlich zu 4, so oft D entweder $\equiv 0$ oder $\equiv 3$ (mod. 4) ist, und zu 8, so oft D entweder $\equiv 0$ oder $\equiv 2$ oder $\equiv 6$ (mod. 8) ist.*) Eine derartige Beziehung zu diesen einzelnen Zahlen werden wir den **Character** oder **Specialcharacter** der Form F nennen und dieselbe auf folgende Weise ausdrücken: Wenn nur quadratische Reste der Primzahl p durch die Form F dargestellt werden können, werden wir ihr den Character Rp, im entgegengesetzten Falle den Character Np beilegen; analog werden wir 1,4 schreiben, wenn durch die Form F keine andern ungeraden Zahlen dargestellt werden

---

*) Für die durch 8 teilbaren Determinanten kann man von der Beziehung zu 4 absehen, da sie in diesem Falle schon unter der Beziehung zu 8 enthalten ist.

können als solche, welche $\equiv 1 \pmod{4}$ sind, woraus sogleich hervorgeht, welche Charactere durch die Bezeichnungen 3, 4; 1, 8; 3, 8; 5, 8; 7, 8 ausgedrückt werden. Schliesslich werden wir den Formen, durch welche nur solche ungerade Zahlen dargestellt werden können, welche nach dem Modul 8 entweder $\equiv 1$ oder $\equiv 7$ sind, den Character 1 u. 7, 8 beilegen, woraus sich die Bedeutung der Charactere: 3 u. 5, 8; 1 u. 3, 8; 5 u. 7, 9 von selbst ergiebt.

Die einzelnen Charactere einer gegebenen primitiven Form (a, b, c) mit der Determinante D lassen sich stets wenigstens aus einer der Zahlen a, c (welche offenbar beide durch jene Form darstellbar sind) erkennen. Denn so oft p ein Primteiler von D ist, wird sicher eine der Zahlen a, c durch p nicht teilbar sein; denn wenn beide durch p teilbar wären, würde p auch in b^2 $(= D + ac)$ und somit auch in b aufgehen, d. h. die Form (a, b, c) würde nicht primitiv sein. In analoger Weise würde in denjenigen Fällen, in welchen die Form (a, b, c) zur Zahl 4 oder 8 eine feste Beziehung hat, sicher mindestens eine der Zahlen a, c ungerade sein, woraus somit jene Beziehung erkannt werden kann. So ergiebt sich z. B. für die Form (7, 0, 23) in Bezug auf die Zahl 23 aus der Zahl 7 der Character $N23$; in Bezug auf die Zahl 7 erhält man für dieselbe Form aus der Zahl 23 den Character $R7$; endlich kann der Character dieser Form in Bezug auf die Zahl 4, nämlich 3, 4, sowohl aus der Zahl 7 als auch aus der Zahl 23 erhalten werden.

Da sämtliche Zahlen, welche durch irgend eine in der Klasse K enthaltene Form F dargestellt werden können, auch durch jede andere Form dieser Klasse darstellbar sind, so werden offenbar die einzelnen Charactere der Form F auch allen übrigen Formen dieser Klasse zukommen, weshalb man jene als Charactere der ganzen Klasse betrachten darf. Demnach lassen sich die einzelnen Charactere jeder beliebigen gegebenen primitiven Klasse aus der sie repräsentierenden Form erkennen. Entgegengesetzte Klassen werden stets sämtliche Charactere gemeinsam haben.

231.

Die Gesamtheit aller Specialcharactere einer gegebenen Form oder Klasse bildet den **Totalcharacter** dieser Form oder Klasse. So ist z. B. der Totalcharacter der Form (10, 3, 17) oder der ganzen durch sie repräsentierten Klasse: 1, 4; $N7$; $N23$. In ähnlicher Weise ist der Totalcharacter der Form (7, —1, 17): 7, 8; $R3$; $N5$; denn der Specialcharacter 3, 4 ist in diesem Falle wegzulassen, da er bereits in dem Character 7, 8 enthalten ist. — Hierauf gründen wir die Einteilung der ganzen Ordnung der eigentlich primitiven (falls die Determinante negativ ist, positiven) Klassen mit gegebener Determinante in mehrere verschiedene **Geschlechter**, indem wir alle Klassen, welche denselben Totalcharacter haben, zu demselben Geschlechte, diejenigen aber, deren Totalcharactere verschieden sind, zu verschiedenen

Geschlechtern rechnen. Den einzelnen Geschlechtern aber legen wir diejenigen Totalcharactere bei, welche die in ihnen enthaltenen Klassen haben. So erhält man z. B. für die Determinante — 161 sechzehn eigentlich primitive positive Klassen, welche sich in folgender Weise auf vier Geschlechter verteilen:

Character:	Repräsentierende Formen der Klassen:
1, 4; $R7$; $R23$	(1, 0, 161), (2, 1, 81), (9, 1, 18), (9, —1, 18)
1, 4; $N7$; $N23$	(5, 2, 33), (5, —2, 33), (10, 3, 17), (10, —3, 17)
3, 4; $R7$; $N23$	(7, 0, 23), (11, 2, 15), (11, —2, 15), (14, 7, 15)
3, 4; $N7$; $R23$	(3, 1, 54), (3, —1, 54), (6, 1, 27), (6, —1, 27).

Hinsichtlich der Anzahl der verschiedenen Totalcharactere, so weit sie nämlich a priori möglich sind, *möge man sich Folgendes merken*:

I. *Wenn die Determinante durch 8 teilbar ist*, so sind in Bezug auf die Zahl 8 vier verschiedene Specialcharactere möglich; die Zahl 4 liefert keinen Specialcharacter (Anmerk. zum vorigen Artikel). Ausserdem giebt es in Bezug auf die einzelnen ungeraden Primteiler von D je zwei Charactere. Ist daher die Anzahl jener gleich m, so wird es im Ganzen 2^{m+2} verschiedene Totalcharactere geben (wo $m = 0$ zu setzen ist, wenn D eine Potenz von 2 ist).

II. *Ist die Determinante D nicht durch 8 teilbar, aber durch 4 und ausserdem durch m ungerade Primzahlen*, so hat man im Ganzen 2^{m+1} verschiedene Totalcharactere.

III. *Ist die Determinante D gerade, aber nicht durch 4 teilbar*, so ist sie entweder $\equiv 2$ oder $\equiv 6$ (mod. 8). Im ersten Falle giebt es zwei Specialcharactere hinsichtlich der Zahl 8, nämlich 1 u. 7, 8 und 3 u. 5, 8; im letzteren Falle ebensoviele. Setzt man daher die Anzahl der ungeraden Primteiler von D gleich m, so hat man im Ganzen $2^{(m+1)}$ verschiedene Totalcharactere.

IV. *Ist D ungerade*, so ist sie entweder $\equiv 1$ oder $\equiv 3$ (mod. 4). Im letzteren Falle giebt es hinsichtlich der Zahl 4 zwei verschiedene Charactere, während im ersteren Falle eine solche Beziehung in den Totalcharacter nicht eintritt. Bezeichnet daher m dasselbe wie vorher, so giebt es im ersteren Falle 2^m, im letzeren 2^{m+1} verschiedene Totalcharactere.

Indessen ist wohl zu beachten, dass hieraus keineswegs folgt, dass es in Wirklichkeit ebensoviele Geschlechter gebe, als verschiedene Charactere von vornherein möglich sind. In unserm Beispiel entsprechen nur der Hälfte von diesen wirklich Klassen oder Geschlechter, während es keine positiven Klassen giebt, denen die Charactere 1, 4; $R7$; $N23$ oder 1, 4; $N7$, $R23$ oder 3, 4; $R7$; $R23$ oder 3, 4; $N7$; $N23$ zukommen. Über diesen sehr wichtigen Gegenstand wird unten weitläufiger gehandelt werden.

Die Form (1, 0, $-D$), welche ohne Zweifel unter allen Formen mit der Determinante D für die einfachste zu halten ist, werden wir fortan

Hauptform, die gesamte Klasse, in welcher jene Form vorkommt, **Hauptklasse** und schliesslich das ganze Geschlecht, in welchem die Hauptklasse enthalten ist, **Hauptgeschlecht** nennen. Man muss daher wohl unterscheiden zwischen einer Hauptform, einer Form aus einer Hauptklasse und einer Form aus einem Hauptgeschlecht; ebenso zwischen einer Hauptklasse und einer Klasse aus einem Hauptgeschlecht. Dieser Benennungen werden wir uns stets bedienen, auch wenn es zufällig für irgend eine Determinante andere Klassen ausser der Hauptklasse oder andere Geschlechter ausser dem Hauptgeschlecht nicht giebt, wie dies z. B. meistens der Fall ist, wenn D eine positive Primzahl von der Form $4n+1$ ist.

232.

Obwohl das, was über die Charactere der Formen entwickelt worden ist, zunächst nur zu dem Zwecke angeführt wurde, um die Untereinteilung der positiven eigentlich primitiven Ordnung darauf zu gründen, so steht doch nichts im Wege, dasselbe auch auf negative oder auf uneigentlich primitive Formen und Klassen auszudehnen und sowohl die positive uneigentlich primitive Ordnung als auch die negative eigentlich primitive Ordnung, als auch die negative uneigentlich primitive Ordnung nach demselben Prinzipe in Geschlechter einzuteilen. So kann z. B., nachdem die eigentlich primitive Ordnung der Formen mit der Determinante 145 in die beiden folgenden Geschlechter geteilt ist:

*R*5, *R*29	(1, 0, −145), (5, 0, −29)
*N*5, *N*29	(3, 1, −48), (3, −1, −48),

auch die uneigentlich primitive Ordnung in gleicher Weise in die beiden Geschlechter geteilt worden:

*R*5, *R*29	(4, 1, −36), (4, −1, −36)
*N*5, *N*29	(2, 1, −72), (10, 5, −12);

oder, ebenso wie die positiven Klassen der Formen mit der Determinante −129 in die vier Geschlechter zerfallen:

1,4; *R*3; *R*43	(1, 0, 129), (10, 1, 13), (10, −1, 13)
1,4; *N*3; *N*43	(2, 1, 65), (5, 1, 26), (5, −1, 26)
3,4; *R*3; *N*43	(3, 0, 43), (7, 2, 19), (7, −2, 19)
3,4; *N*4; *R*43	(6, 3, 23), (11, 5, 14), (11, −5, 14),

so scheiden sich auch die negativen Klassen in die vier Geschlechter:

3,4; *N*3; *N*43	(−1, 0, −129), (−10, 1, −13), (−10, −1, −13)
3,4; *R*3; *R*43	(−2, 1, −65), (−5, 1, −26), (−5, −1, −26)
1,4; *N*3; *R*43	(−3, 0, −43), (−7, 2, −19), (−7, −2, −19)
1,4; *R*3; *N*43	(−6, 3, −23), (−11, 5, −14), (−11, −5, −14).

Da jedoch das System der negativen Klassen dem System der positiven Klassen stets ebenso ähnlich ist, dürfte es in den meisten Fällen überflüssig

sein, jenes noch besonders aufzustellen. Wie man aber eine uneigentlich primitive Ordnung auf eine eigentlich primitive zurückführen kann, werden wir später zeigen.

Was schliesslich die abgeleiteten Ordnungen betrifft, so sind für die Untereinteilung derselben neue Regeln nicht erforderlich. Denn da jede abgeleitete Ordnung aus irgend einer primitiven Ordnung (von kleinerer Determinante) entsteht, und die einzelnen Klassen jener sich von selbst nach den einzelnen Klassen dieser richten, so kann offenbar die Untereinteilung einer abgeleiteten Ordnung aus der Untereinteilung der primitiven Ordnung hergeleitet werden.

233.

Wenn die (primitive) Form $F=(a,b,c)$ derart beschaffen ist, dass sich zwei Zahlen g, h finden lassen, für welche $g^2\equiv a$, $gh\equiv b$, $h^2\equiv c$ nach einem gegebenen Modul m wird, so werden wir jene Form den quadratischen Rest der Zahl m und $gx+hy$ einen Wert des Ausdrucks $\sqrt{ax^2+2bxy+cy^2}$ (mod. m) oder kürzer (g, h) einen Wert des Ausdrucks $\sqrt{(a,\ b,\ c)}$ oder $\sqrt{F}$ (mod. m) nennen. Allgemeiner werden wir, wenn der zum Modul m prime Multiplikator M von solcher Beschaffenheit ist, dass

$$g^2\equiv aM,\quad gh\equiv bM,\quad h^2\equiv cM\,(\text{mod. } m)$$

gemacht werden kann, sagen, es sei $M\times(a,\ b,\ c)$ oder MF quadratischer Rest von m und $(g,\ h)$ ein Wert des Ausdrucks $\sqrt{M(a,\ b,\ c)}$ oder $\sqrt{MF}$ (mod. m). So ist z. B. die Form (3, 1, 54) quadratischer Rest von 23 und (7, 10) ein Wert des Ausdrucks $\sqrt{(3,\ 1,\ 54)}$ (mod. 23); analog ist $(2,\ -4)$ ein Wert des Ausdrucks $\sqrt{5(10,\ 3,\ 17)}$ (mod. 23). Der Nutzen dieser Definitionen wird später gezeigt werden; hier wollen wir nur die folgenden Sätze anführen.

I. Ist $M(a,\ b,\ c)$ quadratischer Rest der Zahl m, so wird diese in der Determinante der Form $(a,\ b,\ c)$ aufgehen. Denn wenn $(g,\ h)$ ein Wert des Ausdrucks $\sqrt{M(a,\ b,\ c)}$ (mod. m) oder

$$g^2\equiv aM,\quad gh\equiv bM,\quad h^2\equiv cM\,(\text{mod. } m)$$

ist, so wird $b^2M^2-acM^2\equiv 0$ oder $(b^2-ac)M^2$ durch m teilbar sein. Da aber M prim zu m vorausgesetzt ist, so wird auch b^2-ac durch m teilbar sein.

II. Ist $M(a,\ b,\ c)$ quadratischer Rest von m und m entweder eine Primzahl oder die Potenz einer Primzahl, etwa gleich p^μ, so wird der Specialcharacter der Form $(a,\ b,\ c)$ in Bezug auf die Zahl p entweder Rp oder Np sein, je nachdem M Rest oder Nichtrest von p ist. Dies folgt sogleich daraus, dass sowohl aM als auch cM quadratischer Rest von m oder von p und mindestens eine der Zahlen a, c nicht durch p teilbar ist (Artikel 230).

In analoger Weise ist, wenn $m = 4$ ist (während das übrige ungeändert bleibt), entweder 1,4 oder 3,4 der Specialcharacter der Form (a, b, c), je nachdem $M \equiv 1$ oder $\equiv 3$ ist; ferner ist, wenn $m = 8$ oder eine höhere Potenz von 2 ist, 1, 8; 3, 8; 5, 8; 7, 8 der Specialcharacter der Form (a, b, c), je nachdem respective $M \equiv 1$; 3; 5; 7 (mod. 8) ist.

III. Umgekehrt, wenn m eine Primzahl oder die Potenz einer ungeraden Primzahl, z. B. p^μ, ist, welche in der Determinante $b^2 - ac$ aufgeht, und ferner M entweder Rest oder Nichtrest von p ist, je nachdem der Character der Form (a, b, c) in Bezug auf p bezüglich Rp oder Np ist, so wird $M(a, b, c)$ quadratischer Rest von m sein. Denn wenn a durch p nicht teilbar ist, so wird aM Rest von p und daher auch von m; wenn daher g ein Wert des Ausdrucks $\sqrt{aM}$ (mod. m), h der Wert des Ausdrucks $\frac{bg}{a}$ (mod. m) ist, so wird $g^2 \equiv aM$, $ah \equiv bg$ und daher:

$$agh \equiv bg^2 \equiv abM \text{ und } gh \equiv bM,$$

endlich

$$ah^2 \equiv bgh \equiv b^2M \equiv b^2M - (b^2 - ac)M \equiv acM$$

und somit $h^2 \equiv cM$, d. h. (g, h) ist ein Wert des Ausdrucks $\sqrt{M(a, b, c)}$. Wenn aber a durch m teilbar ist, so ist es sicher c nicht; hieraus ist leicht ersichtlich, dass man zu demselben Resultat kommt, wenn man für h einen Wert des Ausdrucks $\sqrt{cM}$ (mod. m), für g den Wert des Ausdrucks $\frac{bh}{c}$ (mod. m) nimmt.

In analoger Weise beweist man, dass, wenn $m = 4$ ist und in $b^2 - ac$ aufgeht und wenn ferner M entweder $\equiv 1$ oder $\equiv 3$ angenommen wird, je nachdem 1, 4 oder 3, 4 der Specialcharacter der Form (a, b, c) ist, $M(a, b, c)$ quadratischer Rest von m sein wird. Ebenso auch, wenn $m = 8$ oder eine höhere Potenz von 2 ist, durch welche $b^2 - ac$ teilbar ist, wenn ferner $M \equiv 1$; 3; 5; 7 (mod. 8) angenommen wird, je nachdem es der Specialcharacter der Form (a, b, c) in Bezug auf die Zahl 8 erfordert, dass $M(a, b, c)$ quadratischer Rest von m ist.

IV. Wenn die Determinante der Form (a, b, c) gleich D und $M(a, b, c)$ quadratischer Rest von D ist, so lassen sich sämtliche Specialcharactere der Form (a, b, c) sowohl in Bezug auf die einzelnen ungeraden Primteiler von D, als auch in Bezug auf die Zahl 4 oder die Zahl 8 (wenn sie in D aufgehen) aus der Zahl M sogleich erkennen. So sind z. B., da 3 (20, 10, 27) quadratischer Rest von 440, nämlich (150, 9) ein Wert des Ausdrucks $\sqrt{3\,(20, 10, 27)}$ (mod. 440) und $3\,N\,5$, $3\,R\,11$ ist, die Charactere der Form (20, 10, 27) die folgenden: 3, 8; $N\,5$; $R\,11$. Nur die Specialcharactere hinsichtlich der Zahlen 4 und 8 haben, sobald diese nicht in der Determinante aufgehen, keinen notwendigen Zusammenhang mit der Zahl M.

V. Umgekehrt, wenn die zu D prime Zahl M sämtliche Specialcharactere der Form (a, b, c) in sich enthält (mit Ausnahme der Charactere

in Bezug auf die Zahlen 4 und 8, falls sie nicht in D aufgehen), so wird $M(a, b, c)$ quadratischer Rest von D sein. Denn aus III ergiebt sich, dass, wenn die Zahl D auf die Form $\pm A^\alpha B^\beta C^\gamma \ldots$ gebracht wird, so dass $A, B, C, \ldots$ verschiedene Primzahlen sind, $M(a, b, c)$ quadratischer Rest der einzelnen Zahlen $A^\alpha, B^\beta, C^\gamma, \ldots$ ist. Wenn daher $(\mathfrak{A}, \mathfrak{A}')$ ein Wert des Ausdrucks $\sqrt{M(a, b, c)}$ nach dem Modul A^α, $(\mathfrak{B}, \mathfrak{B}')$ ein Wert desselben Ausdrucks nach dem Modul B^β, $(\mathfrak{C}, \mathfrak{C}')$ einer nach dem Modul C^γ, u. s. w. ist, und die Zahlen g, h so bestimmt werden, dass $g \equiv \mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$, $h \equiv \mathfrak{A}', \mathfrak{B}', \mathfrak{C}', \ldots$ nach den Moduln $A^\alpha, B^\beta, C^\gamma, \ldots$ respective ist (Artikel 32), so sieht man leicht, dass $g^2 \equiv aM$, $gh \equiv bM$, $h^2 \equiv cM$ nach sämtlichen Moduln $A^\alpha, B^\beta, C^\gamma, \ldots$ ist und daher auch nach dem Modul D, welcher das Product aus jenen ist.

VI. Aus diesen Gründen werden derartige Zahlen wie M die **characteristischen Zahlen** der Form (a, b, c) genannt, und können nach V. mehrere derartige Zahlen ohne Schwierigkeit gefunden werden, sobald sämtliche Specialcharactere dieser Form ermittelt sind; die einfachsten von ihnen lassen sich meistens am leichtesten durch Probieren finden. Offenbar werden, wenn M eine characteristische Zahl einer gegebenen primitiven Form mit der Determinante D ist, alle Zahlen, welche M nach dem Modul D congruent sind, characteristische Zahlen derselben Form sein; ferner haben die Formen in derselben Klasse oder auch die in verschiedenen Klassen desselben Geschlechts enthaltenen dieselben characteristischen Zahlen, weshalb jede characteristische Zahl einer gegebenen Form auch der ganzen Klasse und dem ganzen Geschlecht beigelegt werden kann; endlich ist 1 stets die characteristische Zahl einer Hauptform, Hauptklasse und eines Hauptgeschlechts oder jede Form aus einem Hauptgeschlecht quadratischer Rest von ihrer Determinante.

VII. Ist (g, h) ein Wert des Ausdrucks $\sqrt{M(a, b, c)}$ (mod. m) und $g' \equiv g$, $h' \equiv h$ (mod. m), so ist auch (g', h') ein Wert desselben Ausdrucks. Derartige Werte können als äquivalent betrachtet werden; sind dagegen (g, h), (g', h') Werte des Ausdrucks $\sqrt{M(a, b, c)}$ (mod. m), ist jedoch nicht gleichzeitig $g' \equiv g$, $h' \equiv h$ (mod. m), so sind jene Werte als verschieden zu erachten. Offenbar wird, wenn (g, h) ein Wert eines solchen Ausdrucks ist, auch $(-g, -h)$ ein solcher sein, und man zeigt leicht, dass diese Werte immer verschieden sind, wofern nicht $m = 2$ ist. Ebenso leicht zeigt man, dass der Ausdruck $\sqrt{M(a, b, c)}$ (mod. m) mehr verschiedene Werte als zwei solche (entgegengesetzte) nicht haben kann, wenn m entweder eine ungerade Primzahl oder die Potenz einer ungeraden Primzahl oder gleich 4 ist; dass es aber, wenn $m = 8$ oder eine höhere Potenz von 2 ist, im Ganzen vier solche giebt. Hieraus folgt mit Hülfe von VI. leicht, dass es, wenn die Determinante D der Form (a, b, c) gleich $\pm 2^\mu A^\alpha B^\beta \ldots$ ist, wo $A, B, \ldots$ von einander verschiedene ungerade Primzahlen, deren Anzahl gleich n sei, bezeichnen, und wenn M eine characteristische Zahl jener Form ist, im Ganzen entweder 2^n oder 2^{n+1} oder 2^{n+2} verschiedene Werte des Aus-

drucks $\sqrt{M(a, b, c)}$ (mod. D) giebt, je nachdem μ entweder < 2 oder $= 2$ oder > 2 ist. So erhält man z. B. sechzehn Werte des Ausdrucks $\sqrt{7(12, 6, -17)}$ (mod. 240), nämlich $(\pm 18, \mp 11)$, $(\pm 18, \pm 29)$, $(\pm 18, \mp 91)$, $(\pm 18, \pm 109)$, $(\pm 78, \pm 19)$, $(\pm 78, \pm 59)$, $(\pm 78, \mp 61$, $(\pm 78, \mp 101)$. Einen ausführlicheren Beweis fügen wir der Kürze halber nicht hinzu, da er für das Folgende nicht so notwendig ist.

VIII. Schliesslich bemerken wir, dass, wenn D die Determinante zweier äquivalenten Formen (a, b, c), (a', b', c'), M ihre characteristische Zahl ist und die erste in die zweite übergeht durch die Substitution $\alpha, \beta, \gamma, \delta$, alsdann aus jedem Werte des Ausdrucks $\sqrt{M(a, b, c)}$ z. B. aus (g, h) sich ein Wert des Ausdrucks $\sqrt{M(a', b', c')}$ ergiebt, nämlich $(\alpha g + \gamma h, \beta g + \delta h)$. Den Beweis wird jeder ohne Schwierigkeit ableiten können.

Von der Composition der Formen.

234.

Nachdem wir dies über die Einteilung der Formen in Klassen, Geschlechter und Ordnungen vorausgeschickt und die allgemeinen Eigenschaften, welche sich aus diesen Unterscheidungen unmittelbar ergeben, entwickelt haben, gehen wir zu einem andern sehr wichtigen, bisher noch von Niemand berührten Gegenstande, nämlich der Composition der Formen, über. Am Beginn dieser Untersuchung schieben wir sogleich, um nicht nachher die fortlaufende Reihe der Beweise unterbrechen zu müssen, ein den folgenden

Hülfssatz. Hat man vier Reihen ganzer Zahlen:

$$a, a', a'', \ldots, a^{(n)};\ b, b', b'', \ldots, b^{(n)};\ c, c', c'', \ldots, c^{(n)};\ d, d', d'', \ldots, d^{(n)},$$

welche aus gleich vielen (nämlich $n+1$) Gliedern bestehen und so beschaffen sind, dass

$$cd' - dc',\ cd'' - dc'', \ldots,\ c'd'' - d'c'', \ldots.$$

respective gleich

$$k(ab' - ba'),\ k(ab'' - ba''), \ldots,\ k(a'b'' - b'a''), \ldots.$$

sind, oder dass allgemein

$$c^{(\lambda)}d^{(\mu)} - d^{(\lambda)}c^{(\mu)} = k(a^{(\lambda)}b^{(\mu)} - b^{(\lambda)}a^{(\mu)})$$

ist, wo k eine gegebene ganze Zahl ist und λ, μ irgend welche von einander verschiedene ganze Zahlen zwischen 0 und n incl. sind, deren grössere μ sei*), und ausserdem sämtliche $a^{(\lambda)}b^{(\mu)} - b^{(\lambda)}a^{(\mu)}$

*) Indem man a als a^0, b als b^0 u. s. w. betrachtet. — Übrigens wird offenbar dieselbe Gleichung gelten, auch wenn $\lambda = \mu$ oder $\lambda > \mu$ ist.

keinen gemeinschaftlichen Teiler haben, so lassen sich vier ganze Zahlen α, β, γ, δ von der Art finden, dass

$$\alpha a+\beta b=c,\quad \alpha a'+\beta b'=c',\quad \alpha a''+\beta b''=c'',\ldots$$
$$\gamma a+\delta b=d,\quad \gamma a'+\delta b'=d',\quad \gamma a''+\delta b''=d'',\ldots$$

oder allgemein

$$\alpha a^{(\nu)}+\beta b^{(\nu)}=c^{(\nu)},\quad \gamma a^{(\nu)}+\delta b^{(\nu)}=d^{(\nu)}$$

ist. Ist dies geschehen, so ist:

$$\alpha\delta-\beta\gamma=k.$$

Da nach Voraussetzung die Zahlen $ab'-ba'$, $ab''-ba''$, ..., $a'b''-b'a''$, ... (deren Anzahl gleich $\frac{1}{2}n(n+1)$ ist) keinen gemeinschaftlichen Teiler haben, so lassen sich ebenso viele andere ganze Zahlen finden, so dass, wenn man jene mit diesen respective multipliciert, die Summe der Producte gleich 1 wird (Artikel 40). Diese Multiplikatoren mögen mit (0,1), (0,2), ... (1,2), ... oder allgemein der Multiplikator von $a^{(\lambda)}b^{(\mu)}-b^{(\lambda)}a^{(\mu)}$ mit (λ,μ) bezeichnet werden, so dass

$$\Sigma(\lambda,\mu)\,(a^{(\lambda)}b^{(\mu)}-b^{(\lambda)}a^{(\mu)})=1$$

ist. (Durch den Buchstaben Σ bezeichnen wir das Aggregat aller Werte des nachfolgenden Ausdrucks, welche dadurch entstehen, dass man λ, μ alle verschiedenen Werte zwischen 0 und n, bei denen $\mu>\lambda$ ist, beilegt.) Setzt man hierauf:

$$\Sigma(\lambda,\mu)\,(c^{(\lambda)}b^{(\mu)}-b^{(\lambda)}c^{(\mu)})=\alpha,\quad \Sigma(\lambda,\mu)\,(a^{(\lambda)}c^{(\mu)}-c^{(\lambda)}a^{(\mu)})=\beta$$
$$\Sigma(\lambda,\mu)\,(d^{(\lambda)}b^{(\mu)}-b^{(\lambda)}d^{(\mu)})=\gamma,\quad \Sigma(\lambda,\mu)\,(a^{(\lambda)}d^{(\mu)}-d^{(\lambda)}a^{(\mu)})=\delta,$$

so werden diese Zahlen α, β, γ, δ die vorgeschriebenen Eigenschaften besitzen.

Beweis. I. Bezeichnet ν irgend eine ganze Zahl zwischen 0 und n, so ist:

$$\begin{aligned}\alpha a^{(\nu)}+\beta b^{(\nu)}&=\Sigma(\lambda,\mu)\,(c^{(\lambda)}b^{(\mu)}a^{(\nu)}-b^{(\lambda)}c^{(\mu)}a^{(\nu)}+a^{(\lambda)}c^{(\mu)}b^{(\nu)}-c^{(\lambda)}a^{(\mu)}b^{(\nu)})\\&=\frac{1}{k}\Sigma(\lambda,\mu)\,(c^{(\lambda)}d^{(\mu)}c^{(\nu)}-d^{(\lambda)}c^{(\mu)}c^{(\nu)})\\&=\frac{1}{k}c^{(\nu)}\Sigma(\lambda,\mu)\,(c^{(\lambda)}d^{(\mu)}-d^{(\lambda)}c^{(\mu)})\\&=c^{(\nu)}\Sigma(\lambda,\mu)\,(a^{(\lambda)}b^{(\mu)}-b^{(\lambda)}a^{(\mu)})\\&=c^{(\nu)}\end{aligned}$$

Und durch analoge Rechnung findet man:

$$\gamma a^{(\nu)}+\delta b^{(\nu)}=d^{(\nu)}.$$

II. Da somit

$$c^{(\lambda)}=\alpha a^{(\lambda)}+\beta b^{(\lambda)},\qquad c^{(\mu)}=\alpha a^{(\mu)}+\beta b^{(\mu)}$$

ist, so wird:

$$c^{(\lambda)}b^{(\mu)} - b^{(\lambda)}c^{(\mu)} = \alpha(a^{(\lambda)}b^{(\mu)} - b^{(\lambda)}a^{(\mu)})$$

und analog:

$$a^{(\lambda)}c^{(\mu)} - c^{(\lambda)}a^{(\mu)} = \beta(a^{(\lambda)}b^{(\mu)} - b^{(\lambda)}a^{(\mu)})$$
$$d^{(\lambda)}b^{(\mu)} - b^{(\lambda)}d^{(\mu)} = \gamma(a^{(\lambda)}b^{(\mu)} - b^{(\lambda)}a^{(\mu)})$$
$$a^{(\lambda)}d^{(\mu)} - d^{(\lambda)}a^{(\mu)} = \delta(a^{(\lambda)}b^{(\mu)} - b^{(\lambda)}a^{(\mu)}),$$

und aus diesen Formeln lassen sich die Werte von α, β, γ, δ viel leichter finden, wenn man nur λ, μ so annimmt, dass $a^{(\lambda)}b^{(\mu)} - b^{(\lambda)}a^{(\mu)}$ nicht gleich 0 ist, was sicher möglich ist, weil nach Voraussetzung nicht alle $a^{(\lambda)}b^{(\mu)} - b^{(\lambda)}a^{(\mu)}$ einen gemeinschaftlichen Teiler haben und daher nicht sämtlich gleich 0 sein können. — Aus eben diesen Gleichungen ergiebt sich, wenn man die erste mit der vierten, die zweite mit der dritten multipliciert und subtrahiert:

$$(\alpha\delta - \beta\gamma)\,(a^{(\lambda)}b^{(\mu)} - b^{(\lambda)}a^{(\mu)})^2 = (a^{(\lambda)}b^{(\mu)} - b^{(\lambda)}a^{(\mu)})\,(c^{(\lambda)}d^{(\mu)} - d^{(\lambda)}c^{(\mu)})$$
$$= k\,(a^{(\lambda)}b^{(\mu)} - b^{(\lambda)}a^{(\mu)})^2,$$

und daher notwendig:

$$\alpha\delta - \beta\gamma = k.$$

235.

Wenn die Form

$$AX^2 + 2BXY + CY^2 = F$$

übergeht in das Product zweier Formen:

$$ax^2 + 2bxy + cy^2 = f, \qquad a'x'^2 + 2b'x'y' + c'y'^2 = f'$$

durch eine Substitution von der Form:

$$X = pxx' + p'xy' + p''yx' + p'''yy'$$
$$Y = qxx' + q'xy' + q''yx' + q'''yy'$$

(was wir der Kürze halber im Folgenden stets so ausdrücken werden: Wenn F in ff' übergeht durch die Substitution p, p', p'', p'''; q, q', q'', q''')*), so werden wir einfach sagen, die Form F sei **transformierbar** in ff'; ist diese Transformation überdies so beschaffen, dass die sechs Zahlen

$$pq' - qp',\; pq'' - qp'',\; pq''' - qp''',\; p'q'' - q'p'',\; p'q''' - q'p''',\; p''q''' - q''p'''$$

*) Bei dieser Bezeichnung hat man also auf die Reihenfolge sowohl der Coefficienten p, p', ... als auch der Formen f, f' wohl zu achten. Man sieht aber leicht, dass, wenn man die Reihenfolge der Formen f, f' derart ändert, dass die erste zur zweiten wird, die Coefficienten p', q' mit p'', q'' zu vertauschen sind, jeder der übrigen aber an seinem Platze bleibt.

keinen gemeinschaftlichen Teiler haben, so werden wir die Form F aus den Formen f, f' **zusammengesetzt (componiert)** nennen.

Wir werden unsere Untersuchung mit der allgemeinsten Annahme beginnen, nämlich dass F in ff' durch die Substitution $p, p', p'', p'''; q, q', q'', q'''$ übergeht, und wollen entwickeln, was daraus folgt. Offenbar werden dieser Annahme die folgenden neun Gleichungen völlig äquivalent sein (d. h. sobald diese Gleichungen stattfinden, wird die Form F durch die genannnte Substitution in ff' übergehen und umgekehrt):

[1] $$Ap^2 + 2Bpq + Cq^2 = aa'$$
[2] $$Ap'^2 + 2Bp'q' + Cq'^2 = ac'$$
[3] $$Ap''^2 + 2Bp''q'' + Cq''^2 = ca'$$
[4] $$Ap'''^2 + 2Bp'''q''' + Cq'''^2 = cc'$$
[5] $$App' + B(pq' + qp') + Cqq' = ab'$$
[6] $$App'' + B(pq'' + qp'') + Cqq'' = ba'$$
[7] $$Ap'p''' + B(p'q''' + q'p''') + Cq'q''' = bc'$$
[8] $$Ap''p''' + B(p''q''' + q''p''') + Cq''q''' = cb'$$
[9] $$A(pp''' + p'p'') + B(pq''' + qp''' + p'q'' + q'p'') + C(qq''' + q'q'') = 2bb'.$$

Es seien die Determinanten der Formen F, f, f' respective D, d, d', die grössten gemeinschaftlichen Teiler der Zahlen A, $2B$, C; a, $2b$, c; a', $2b'$, c' respective M, m, m' (die wir als positiv genommen voraussetzen); ferner bestimme man sechs ganze Zahlen $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$ derart, dass

$$\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m, \quad \mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c' = m'$$

ist; endlich bezeichne man die Zahlen

$$pq' - qp',\ pq'' - qp'',\ pq''' - qp''',\ p'q'' - q'p'',\ p'q''' - q'p''',\ p''q''' - q''p'''$$

respective mit P, Q, R, S, T, U, und deren grössten gemeinschaftlichen positiv genommenen Teiler mit k. — Setzt man dann:

[10] $$App''' + B(pq''' + qp''') + Cqq''' = bb' + \Delta,$$

so wird nach Gleichung [9]:

[11] $$Ap'p'' + B(p'q'' + q'p'') + Cq'q'' = bb' - \Delta.$$

Aus diesen elf Gleichungen [1] bis [11] leiten wir die folgenden neuen Gleichungen her*):

*) Diese Gleichungen entstehen so: [12] aus $[5]^2 - [1]\cdot[2]$; [13] aus $[5]\cdot[9] - [1]\cdot[7] - [2]\cdot[6]$; [14] aus $[10]\cdot[11] - [6]\cdot[7]$; [15] aus $[5]\cdot[8] + [5]\cdot[8] + [10]^2 - [11]^2 - [1]\cdot[4] - [2]\cdot[3] - [6]\cdot[7] - [6]\cdot[7]$; [16] aus $[8]\cdot[9] - [3]\cdot[7] - [4]\cdot[6]$; [17] aus $[8]^2 - [3]\cdot[4]$. Die Ableitung der übrigen sechs geschieht in derselben Weise, wenn man nur die Gleichungen [2], [5], [7] mit den Gleichungen [3], [6], [8] resp. vertauscht und die andern [1], [4], [9], [10], [11] der Reihe nach an ihrem Platze lässt, nämlich [18] aus $[6]^2 - [1]\cdot[3]$, u. s. w.

$$
\begin{aligned}
&[12] && DP^2 = d'a^2 \\
&[13] && DP(R-S) = 2d'ab \\
&[14] && DPU = d'ac - (\Delta^2 - dd') \\
&[15] && D(R-S)^2 = 4d'b^2 + 2(\Delta^2 - dd') \\
&[16] && D(R-S)U = 2d'bc \\
&[17] && DU^2 = d'c^2 \\
&[18] && DQ^2 = da'^2 \\
&[19] && DQ(R+S) = 2da'b' \\
&[20] && DQT = da'c' - (\Delta^2 - dd') \\
&[21] && D(R+S)^2 = 4db'^2 + 2(\Delta^2 - dd') \\
&[22] && D(R+S)T = 2db'c' \\
&[23] && DT^2 = dc'^2.
\end{aligned}
$$

Aus diesen folgen wiederum die beiden:

$$
\begin{aligned}
0 &= 2d'a^2(\Delta^2 - dd') \\
0 &= (\Delta^2 - dd')^2 - 2d'ac(\Delta^2 - dd'),
\end{aligned}
$$

nämlich die erste aus [12]·[15] — [13]·[13], die zweite aus [14]·[14] — [12]·[17], und hieraus ist leicht ersichtlich, dass notwendig $\Delta^2 - dd' = 0$ ist, mag a gleich Null sein oder nicht.*) Wir setzen daher voraus, dass auf den rechten Seiten der Gleichungen [14], [15], [20], [21] der Ausdruck $\Delta^2 - dd'$ fehle.

Setzt man jetzt:

$$
\begin{aligned}
\mathfrak{A}P + \mathfrak{B}(R-S) + \mathfrak{C}U &= mn' \\
\mathfrak{A}'Q + \mathfrak{B}'(R+S) + \mathfrak{C}'T &= m'n
\end{aligned}
$$

(wobei wohl zu beachten ist, dass n, n' auch Brüche sein können, obwohl mn', $m'n$ notwendig ganz sind), so folgt leicht aus den Gleichungen [12] bis [17]:

$$Dm^2n'^2 = d'(\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c)^2 = d'm^2$$

und analog aus den Gleichungen [18] bis [23]:

$$Dm'^2n^2 = d(\mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c')^2 = dm'^2.$$

Es ist daher $d = Dn^2$, $d' = Dn'^2$, woraus wir als **erste Folgerung** erhalten: Die Determinanten der Formen F, f, f' stehen notwendig in dem Verhältnis von Quadratzahlen zu einander, und als **zweite Folgerung**: D geht stets in den Zahlen dm'^2, $d'm^2$ ohne Rest auf. Hieraus geht hervor, dass D, d, d' dasselbe Zeichen haben, und dass keine Form in das Product ff' transformierbar ist, deren Determinante grösser ist, als der grösste gemeinschaftliche Teiler der Zahlen dm'^2, $d'm^2$.

Multipliciert man die Gleichungen [12], [13], [14], ebenso auch die Gleichungen [13], [15], [16] sowie [14], [16], [17] respective mit $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$,

---

*) Diese Ableitung der Gleichung $\Delta^2 = dd'$ genügt zum vorliegenden Zwecke; sonst hätten wir ein eleganteres, hier aber zu weitläufiges Verfahren angeben können, um aus den Gleichungen [1] bis [11] die Gleichung $0 = (\Delta^2 - dd')^2$ direct abzuleiten.

addiert die jedesmaligen drei Prodncte, dividiert die Summe durch Dmn' und schreibt Dn'^2 für d', so erhält man:

$$P = an', \quad R - S = 2bn', \quad U = cn'.$$

Auf analoge Weise erhält man, wenn man die Gleichungen [18], [19], [20], ferner [19], [21], [22] sowie [20], [22], [23] respective mit $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$ multipliciert:

$$Q = a'n, \quad R + S = 2b'n, \quad T = c'n.$$

Hieraus erhält man als **dritte Folgerung**: Die Zahlen a, $2b$, c sind proportional den Zahlen P, $R - S$, U, und wenn man das Verhältnis jener zu diesen gleich $1:n'$ setzt, so ist n' die Quadratwurzel aus $\frac{d'}{D}$; ebenso haben die Zahlen a', $2b'$, c' zu Q, $R + S$, T dasselbe Verhältnis und wenn man dasselbe gleich $1:n$ setzt, so ist n die Quadratwurzel aus $\frac{d}{D}$.

Übrigens können die Grössen n, n' sowohl die positiven als auch die negativen Quadratwurzeln von $\frac{d}{D}$, $\frac{d'}{D}$ sein, worauf wir eine Unterscheidung gründen, die beim ersten Anblick zwecklos erscheint, deren Nutzen aber im Folgenden hinreichend zu Tage treten wird. Wir werden nämlich sagen, bei der Transformation der Form F in ff' werde die Form f **direct genommen,** wenn n positiv, **invers,** wenn n negativ ist, und analog werde f' direct oder invers genommen, je nachdem n' positiv oder negativ ist. Tritt aber die Bedingung hinzu, dass $k = 1$ sei, so heisst die Form F entweder aus beiden Formen f, f' direct, oder aus beiden invers, oder aus f direct und aus f' invers, oder aus f invers und aus f' direct zusammengesetzt, je nachdem entweder beide Zahlen n, n' positiv, oder beide negativ, oder die erste positiv und die zweite negativ, oder die erste negativ und die zweite positiv ist. Übrigens wird jeder leicht erkennen, dass diese Beziehungen von der Reihenfolge, in welcher f, f' aufeinanderfolgen (Vgl. die erste Anmerkung zu diesem Artikel), nicht abhängen.

Ferner bemerken wir, dass der grösste gemeinschaftliche Teiler der Zahlen P, Q, R, S, T, U nämlich k in den Zahlen mn', $m'n$ (wie aus den oben abgeleiteten Werten hervorgeht) und daher das Quadrat k^2 in $m^2n'^2$, m'^2n^2 und Dk^2 in $d'm^2$, dm'^2 aufgeht. Aber auch umgekehrt wird jeder gemeinschaftliche Teiler von mn', $m'n$ in k aufgehen. Denn es sei e ein solcher Teiler, der offenbar auch in den Zahlen an', $2bn'$, cn', $a'n$, $2b'n$, $c'n$ d. h. auch in den Zahlen P, $R - S$, U, Q, $R + S$, T und folglich auch in $2R$ und $2S$ aufgehen wird. Wäre nun $\frac{2R}{e}$ eine ungerade Zahl, so würde auch $\frac{2S}{e}$ eine ungerade Zahl sein müssen (da die Summe und Differenz

gerade Zahlen sind) und somit würde auch ihr Product ungerade sein. Dieses Product ist aber gleich $\frac{4}{e^2}(b'^2n^2 - b^2n'^2) = \frac{4}{e^2}(d'n^2 + a'c'n^2 - dn'^2 - acn'^2)$ $= \frac{4}{e^2}(a'c'n^2 - acn'^2)$ und daher gerade, weil e in $a'n$, $c'n$, an', cn' aufgeht. Daher ist $\frac{2R}{e}$ notwendig gerade und daher R und ebenso S durch e teilbar. Da somit e in allen sechs Zahlen P, Q, R, S, T, U aufgeht, so wird es auch in ihrem grössten gemeinschaftlichen Teiler k aufgehen. — Hieraus folgt, dass k der grösste gemeinschaftliche Teiler der Zahlen mn', $m'n$ ist, woraus leicht ersichtlich ist, dass Dk^2 der grösste gemeinschaftliche Teiler der Zahlen dm'^2, $d'm^2$ ist. Dies ist die **vierte Folgerung**. Offenbar also wird, wenn F aus f und f' zusammengesetzt ist, D der grösste gemeinschaftliche Teiler der Zahlen dm'^2 und $d'm^2$ sein und umgekehrt, und diese Eigenschaft kann auch als Definition einer zusammengesetzten Form genommen werden. Eine aus den Formen f, f' zusammengesetzte Form hat demnach unter allen Formen, welche in das Product ff' transformierbar sind, die grösstmögliche Determinante.

Bevor wir weiter vorschreiten können, müssen wir vor Allem den Wert von Δ, der, wie wir gezeigt haben, gleich $\sqrt{dd'} = \sqrt{D^2n^2n'^2}$ ist, dessen Vorzeichen aber bisher noch nicht bestimmt worden ist, genauer definieren. Zu diesem Zwecke leiten wir aus den Fundamentalgleichungen [1] bis [11] die Gleichung her: $DPQ = \Delta aa'$ (die aus $[5]\cdot[6] - [1]\cdot[11]$ erhalten wird) und somit: $Daa'nn' = \Delta aa'$, woraus, wenn nicht eine der Zahlen a, a' gleich 0 ist, folgt: $\Delta = Dnn'$. Aber in genau derselben Weise lassen sich aus den Fundamentalgleichungen acht andere Gleichungen ableiten, bei denen auf der linken Selte Dnn' und auf der rechten Δ multipliciert sind mit $2ab'$, ac', $2ba'$, $4bb'$, $2bc'$, ca', $2cb'$, cc'*), woraus, weil weder alle a, $2b$, c, noch alle a', $2b'$, c' gleich 0 sein können, leicht folgt, dass in allen Fällen $\Delta = Dnn'$ wird und daher Δ dasselbe Zeichen hat wie D, d, d' oder das entgegengesetzte, je nachdem n, n' dasselbe oder verschiedenes Vorzeichen haben.

Ferner bemerken wir, dass die Zahlen aa', $2ab'$, ac', $2ba'$, $4bb'$, $2bc'$, ca', $2cb'$, cc', $2bb' + 2\Delta$, $2bb' - 2\Delta$ sämtlich durch mm' teilbar sind. Von den neun ersten ist dies an sich klar, von den beiden andern aber kann dies auf ähnliche Weise bewiesen werden, wie wir oben zeigten, dass R und S durch e teilbar sind. Offenbar nämlich sind $4bb' + 4\Delta$ und $4bb' - 4\Delta$ durch mm' teilbar (da $4\Delta = \sqrt{16dd'}$ und $4d$ durch m^2, $4d'$ durch m'^2 und somit $16dd'$ durch $m^2m'^2$ und 4Δ durch mm' teilbar ist) und die Differenz der Quotienten eine gerade Zahl; man zeigt aber leicht, dass das Product aus

*) Die Ableitung, die der Leser leicht selbst wird finden können, müssen wir der Kürze halber unterdrücken.

den Quotienten eine gerade Zahl ist, woraus folgt, dass jeder der beiden Quotienten gerade und $2bb'+2\Delta$ sowie $2bb'-2\Delta$ durch mm' teilbar ist.

Aus den elf Fundamentalgleichungen leitet man nun leicht die folgenden sechs Gleichungen her:

$$\begin{aligned}
AP^2 &= aa'q'^2 - 2ab'qq' + ac'q^2\\
AQ^2 &= aa'q''^2 - 2ba'qq'' + ca'q^2\\
AR^2 &= aa'q'''^2 - 2(bb'+\Delta)qq''' + cc'q^2\\
AS^2 &= ac'q''^2 - 2(bb'-\Delta)q'q'' + ca'q'^2\\
AT^2 &= ac'q'''^2 - 2bc'q'q''' + cc'q'^2\\
AU^2 &= ca'q'''^2 - 2cb'q''q''' + cc'q''^2.
\end{aligned}$$

Demnach sind sämtliche Grössen AP^2, AQ^2, ... durch mm' teilbar, woraus, da k^2 der grösste gemeinschaftliche Teiler der Zahlen P^2, Q^2, R^2, ... ist, leicht folgt, dass auch Ak^2 durch mm' teilbar ist. Substituiert man aber für a, $2b$, c, a', $2b'$, c' ihre Werte $\frac{P}{n'}$, ... oder $\frac{1}{n'}(pq'-qp')$, ..., so gehen diese Gleichungen in sechs andere über, in denen auf den rechten Seiten die Producte aus der Grösse $\frac{1}{nn'}(q'q''-qq''')$ und den Zahlen P^2, Q^2, R^2, ... stehen. Die sehr einfache Rechnung überlassen wir dem Leser. Hieraus ergiebt sich (da nicht alle Grössen P^2, Q^2, ... gleich 0 sein können): $Ann'=q'q''-qq'''$.

Auf analoge Weise leitet man aus den Fundamentalgleichungen sechs andere Gleichungen her, welche sich von den vorstehenden nur dadurch unterscheiden, dass für A überall C und für q, q', q'', q''' respective p, p', p'', p''' steht, und die wir der Kürze halber nicht herschreiben. Aus diesen folgt in derselben Weise, dass Ck^2 durch mm' teilbar und $Cnn'=p'p''-pp'''$ ist.

Schliesslich fliessen aus derselben Quelle die folgenden sechs Gleichungen:

$$\begin{aligned}
BP^2 &= -aa'p'q' + ab'(pq'+qp') - ac'pq\\
BQ^2 &= -aa'p''q'' + ba'(pq''+qp'') - ca'pq\\
BR^2 &= -aa'p'''q''' + (bb'+\Delta)(pq'''+qp''') - cc'pq\\
BS^2 &= -ac'p''q'' + (bb'-\Delta)(p'q''+q'p'') - ca'p'q'\\
BT^2 &= -ac'p'''q''' + bc'(p'q'''+q'p''') - cc'p'q'\\
BU^2 &= -ca'p'''q''' + cb'(p''q'''+q''p''') - cc'p''q'',
\end{aligned}$$

aus denen ebenso wie vorher folgt, dass $2Bk^2$ durch mm' teilbar und $2Bnn'=pq'''+qp'''-p'q''-q'p''$ ist.

Da nun also Ak^2, $2Bk^2$, Ck^2 durch mm' teilbar sind, so sieht man leicht, dass auch Mk^2 durch mm' teilbar sein muss. Aus den Fundamentalgleichungen ergiebt sich aber, dass M in aa', $2ab'$, ac', $2ba'$, $4bb'$, $2bc'$, ca', $2cb'$, cc' und daher auch in am', $2bm'$, cm' (welche die grössten gemeinschaftlichen Teiler respective der drei ersten, der drei mittleren und der drei letzten dieser neun Zahlen sind) und schliesslich auch in mm', welches der

grösste gemeinschaftliche Teiler dieser letzten drei Grössen ist, aufgeht. Demnach muss offenbar in dem Falle, wo die Form F aus den Formen f, f' zusammengesetzt oder $k=1$ ist, notwendig $M=mm'$ sein. Dies ist die **fünfte Folgerung**.

Wenn der grösste gemeinschaftliche Teiler der Zahlen A, B, C gleich $\mathfrak{M}$ ist, so ist derselbe entweder gleich M (falls die Form F eigentlich primitiv oder aus einer eigentlich primitiven Form abgeleitet ist) oder gleich $\frac{1}{2}M$ (falls die Form F uneigentlich primitiv oder aus einer uneigentlich primitiven Form abgeleitet ist). Bezeichnet man analog die grössten gemeinschaftlichen Teiler der Zahlen a, b, c; a', b', c' respective mit $\mathfrak{m}$, $\mathfrak{m}'$, so ist $\mathfrak{m}$ entweder $=m$ oder $=\frac{1}{2}m$ und $\mathfrak{m}'$ entweder $=m'$ oder $=\frac{1}{2}m'$. Offenbar geht nun $\mathfrak{m}^2$ in d, $\mathfrak{m}'^2$ in d' und daher $\mathfrak{m}^2\mathfrak{m}'^2$ in dd' oder Δ^2 und $\mathfrak{m}\mathfrak{m}'$ in Δ auf. Hiernach folgt aus den sechs letzten Gleichungen für $BP^2, \ldots$, dass $\mathfrak{m}\mathfrak{m}'$ in Bk^2 und daher (da es auch in Ak^2 und Ck^2 aufgeht) auch in $\mathfrak{M}k^2$ aufgeht. So oft daher F aus f, f' zusammengesetzt ist, geht $\mathfrak{m}\mathfrak{m}'$ in $\mathfrak{M}$ auf. Wenn daher in diesem Falle jede der beiden Formen f, f' eigentlich primitiv oder aus einer eigentlich primitiven Form abgeleitet, oder wenn $\mathfrak{m}\mathfrak{m}'=mm'=M$ ist, wird $\mathfrak{M}=M$ oder also F eine Form gleicher Art sein. Wenn aber unter derselben Voraussetzung entweder jede der beiden Formen f, f' oder wenigstens eine von beiden uneigentlich primitiv oder aus einer uneigentlich primitiven Form abgeleitet ist, z. B. die Form f, so folgt aus den Fundamentalgleichungen, dass aa', $2ab'$, ac', ba', $2bb'$, bc', ca', $2cb'$, cc' und somit auch am', bm', cm' und hiernach auch $\mathfrak{m}m'=\frac{1}{2}mm'=\frac{1}{2}M$ durch $\mathfrak{M}$ teilbar sind. Demnach ist in diesem Falle notwendig $\mathfrak{M}=\frac{1}{2}M$, oder es ist auch die Form F entweder uneigentlich primitiv oder aus einer uneigentlich primitiven Form abgeleitet. Dies macht die **sechste Folgerung** aus.

Schliesslich bemerken wir, dass, wenn das Bestehen der neun Gleichungen

$$an'=P, \quad 2bn'=R-S, \quad cn'=U$$
$$a'n=Q, \quad 2b'n=R+S, \quad c'n=T$$
$$Ann'=q'q''-qq''', \quad 2Bnn'=pq'''+qp'''-p'q''-q'p'', \quad Cnn'=p'p''-pp'''$$

(die wir, da wir im Folgenden öfter auf sie zurückkommen müssen, mit Ω bezeichnen wollen) vorausgesetzt wird, nachdem bisher n, n' als Unbekannte betrachtet wurden, von denen jedoch keine gleich 0 ist, durch Substitution leicht bestätigt werden kann, dass auch die Fundamentalgleichungen [1] bis [9] notwendig gelten, oder dass die Form (A, B, C) durch die Substitution p, p', p'', p'''; q, q', q'', q''' in das Product der Formen (a, b, c), (a', b', c') übergeht und dass ausserdem

$$b^2-ac=n^2(B^2-AC), \quad b'^2-a'c'=n'^2(B^2-AC)$$

ist. Die Rechnung, welche hierherzusetzen zu weitläufig sein würde, überlassen wir dem Fleisse des Lesers.

236.

Aufgabe. Wenn zwei Formen gegeben sind, deren Determinanten entweder gleich sind oder wenigstens in dem Verhältnis zweier Quadratzahlen zu einander stehen, so soll man die aus jenen zusammengesetzte Form finden.

Auflösung. Es seien $(a, b, c) = f$, $(a', b', c') = f'$ die zu componierenden Formen, d, d' ihre Determinanten, die grössten gemeinschaftlichen Factoren der Zahlen a, $2b$, c; a', $2b'$, c' resp. gleich m, m', und der grösste gemeinschaftliche Teiler der Zahlen dm'^2, $d'm^2$, mit demselben Zeichen wie d, d' genommen, gleich D. Dann werden $\frac{dm'^2}{D}$, $\frac{d'm^2}{D}$ zu einander prime positive Zahlen und ihr Product eine Quadratzahl sein; daher sind sie selbst Quadrate (Artikel 21). Demnach sind $\sqrt{\frac{d}{D}}$ und $\sqrt{\frac{d'}{D}}$ rationale Zahlen, die wir gleich n, n' setzen, und zwar werden wir für n den positiven oder negativen Wert nehmen, je nachdem die Form f in die Composition entweder direct oder invers eingehen soll, und ebenso werden wir das Zeichen von n' nach der Art und Weise bestimmen, auf welche f' in die Composition eingehen soll. Es werden daher mn', $m'n$ ganze zu einander prime Zahlen sein, während n, n' auch Brüche sein können. Nachdem dies so geschehen, bemerken wir, dass an', cn', $a'n$, $c'n$, $bn' + b'n$, $bn' - b'n$ ganze Zahlen sind, was hinsichtlich der vier ersten von selbst klar ist (da $an' = \frac{a}{m}mn'$ u. s. w. ist); hinsichtlich der beiden andern aber wird dies in derselben Weise bewiesen, wie oben im vorhergehenden Artikel gezeigt wurde, dass R und S durch e teilbar seien.

Man nehme nun vier ganze Zahlen $\mathfrak{Q}$, $\mathfrak{Q}'$, $\mathfrak{Q}''$, $\mathfrak{Q}'''$ nach Belieben, nur unter der einen Bedingung an, dass die vier in den folgenden Gleichungen (I) auf der linken Seite stehenden Grössen nicht sämtlich gleich 0 werden, und setze:

$$(\mathrm{I})\quad \begin{aligned} \mathfrak{Q}'\,an' + \mathfrak{Q}''\,a'n + \mathfrak{Q}'''(bn' + b'n) &= \mu q \\ -\mathfrak{Q}\,an' + \mathfrak{Q}'''\,c'n - \mathfrak{Q}''\,(bn' - b'n) &= \mu q' \\ \mathfrak{Q}'''cn' - \mathfrak{Q}\,a'n + \mathfrak{Q}'\,(bn' - b'n) &= \mu q'' \\ -\mathfrak{Q}''\,cn' - \mathfrak{Q}'\,c'n - \mathfrak{Q}\,(bn' + b'n) &= \mu q''', \end{aligned}$$

so dass q, q', q'', q''' ganze Zahlen werden, welche keinen gemeinschaftlichen Teiler haben, was erreicht wird, wenn man für μ den grössten gemeinschaftlichen Teiler der vier Zahlen, welche in diesen Gleichungen auf der linken Seite stehen, nimmt. Dann lassen sich somit nach Artikel 40 vier ganze Zahlen $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ von der Beschaffenheit finden, dass

$$\mathfrak{P}q + \mathfrak{P}'q' + \mathfrak{P}''q'' + \mathfrak{P}'''q''' = 1$$

ist. Ist dies geschehen, so bestimme man vier Zahlen p, p', p'', p''' durch die folgenden Gleichungen:

$$\text{(II)}\qquad\begin{aligned}
\mathfrak{P}'\, an' + \mathfrak{P}''\, a'n + \mathfrak{P}'''(bn' + b'n) &= p\\
-\mathfrak{P}\, an' + \mathfrak{P}'''c'n - \mathfrak{P}''\,(bn' - b'n) &= p'\\
\mathfrak{P}'''cn' - \mathfrak{P}\, a'n + \mathfrak{P}'\,(bn' - b'n) &= p''\\
-\mathfrak{P}''\, cn' - \mathfrak{P}'\, c'n - \mathfrak{P}\,(bn' + b'n) &= p'''.
\end{aligned}$$

Endlich setze man:

$$q'q'' - qq''' = Ann',\quad pq''' + qp''' - p'q'' - q'p'' = 2Bnn',\quad p'p'' - pp''' = Cnn'.$$

Alsdann werden A, B, C ganze Zahlen und die Form $(A, B, C) = F$ wird aus den Formen f, f' zusammengesetzt sein.

Beweis. I. Aus den Gleichungen (I) ergeben sich ohne Schwierigkeit die folgenden vier Gleichungen:

$$\text{(III)}\qquad\begin{aligned}
0 &= q'\, cn' - q''\, c'n - q'''(bn' - b'n)\\
0 &= q\, cn' + q'''a'n - q''\,(bn' + b'n)\\
0 &= q'''an' + q\, c'n - q'\,(bn' + b'n)\\
0 &= q''\, an' - q'\, a'n - q\,(bn' - b'n).
\end{aligned}$$

II. Nehmen wir jetzt an, dass ganze Zahlen $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$, $\mathfrak{N}$, $\mathfrak{N}'$ derart bestimmt seien, dass

$$\begin{aligned}
\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c &= m\\
\mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c' &= m'\\
\mathfrak{N}m'n + \mathfrak{N}'mn' &= 1
\end{aligned}$$

ist, so wird:

$$\mathfrak{A}a\mathfrak{N}'n' + 2\mathfrak{B}b\mathfrak{N}'n' + \mathfrak{C}c\mathfrak{N}'n' + \mathfrak{A}'a'\mathfrak{N}n + 2\mathfrak{B}'b'\mathfrak{N}n + \mathfrak{C}'c'\mathfrak{N}n = 1.$$

Hiernach und mit Hülfe der Gleichungen (III) bestätigt man leicht, dass, wenn

$$\begin{aligned}
-q'\, \mathfrak{A}\mathfrak{N}' - q''\, \mathfrak{A}'\mathfrak{N} - q'''(\mathfrak{B}\mathfrak{N}' + \mathfrak{B}'\mathfrak{N}) &= \mathfrak{q}\\
q\, \mathfrak{A}\mathfrak{N}' - q'''\mathfrak{C}'\mathfrak{N} + q''\,(\mathfrak{B}\mathfrak{N}' - \mathfrak{B}'\mathfrak{N}) &= \mathfrak{q}'\\
-q'''\mathfrak{C}\mathfrak{N}' + q\, \mathfrak{A}'\mathfrak{N} - q'\,(\mathfrak{B}\mathfrak{N}' - \mathfrak{B}'\mathfrak{N}) &= \mathfrak{q}''\\
q''\, \mathfrak{C}\mathfrak{N}' + q'\, \mathfrak{C}'\mathfrak{N} + q\,(\mathfrak{B}\mathfrak{N}' + \mathfrak{B}'\mathfrak{N}) &= \mathfrak{q}'''
\end{aligned}$$

gesetzt wird, die Gleichungen gelten:

$$\text{(IV)}\qquad\begin{aligned}
\mathfrak{q}'\, an' + \mathfrak{q}''\, a'n + \mathfrak{q}'''\,(bn' + b'n) &= q\\
-\mathfrak{q}\, an' + \mathfrak{q}'''c'n - \mathfrak{q}''\,(bn' - b'n) &= q'\\
\mathfrak{q}'''cn' - \mathfrak{q}\, a'n + \mathfrak{q}'\,(bn' - b'n) &= q''\\
-\mathfrak{q}''\, cn' - \mathfrak{q}'\, c'n - \mathfrak{q}\,(bn' + b'n) &= q'''.
\end{aligned}$$

So oft $\mu = 1$ ist, sind diese Gleichungen nicht notwendig, vielmehr können an ihrer Stelle die Gleichungen (I), denen sie vollständig analog sind, beibehalten werden. Wenn nun aus den Gleichungen (II), (IV) die Werte von Ann', $2Bnn'$, Cnn' (d. h. der Zahlen $q'q'' - qq''', \ldots$) entwickelt werden, und das, was sich gegenseitig aufhebt, weggelassen wird, so findet man, dass die Teile der einzelnen Werte entweder Producte aus ganzen

Zahlen und nn' oder Producte aus ganzen Zahlen und dn'^2 oder aus ganzen Zahlen und $d'n^2$ sind und dass ausserdem die sämtlichen Bestandteile von $2Bnn'$ den Factor 2 enthalten. Hieraus schliesst man (da $dn'^2 = d'n^2$ und somit $\frac{dn'^2}{nn'} = \frac{d'n^2}{nn'} = \sqrt{dd'}$ ganze Zahlen sind), dass A, B, C ganze Zahlen sind.

III. Substituiert man aus den Gleichungen (II) die Werte von p, p' p'', p''', so bestätigt man leicht mit Hülfe der Gleichungen (III) und der Gleichung

$$\mathfrak{P}q + \mathfrak{P}'q' + \mathfrak{P}''q'' + \mathfrak{P}'''q''' = 1,$$

dass

$$pq' - qp' = an', \quad pq''' - qp''' - p'q'' + q'p'' = 2bn', \quad p''q''' - q''p''' = cn'$$
$$pq'' - qp'' = a'n, \quad pq''' - qp''' + p'q'' - q'p'' = 2b'n, \quad p'q''' - q'p''' = c'n$$

ist, und diese Gleichungen sind identisch mit den sechs ersten von Ω im vorigen Artikel; die drei übrigen aber finden bereits infolge der Voraussetzung statt. Daher geht (vgl. den Schluss des vorigen Artikels) die Form F durch die Substitution $p, p', p'', p'''; q, q', q'', q'''$ in ff' über und ihre Determinante ist gleich D oder gleich dem grössten gemeinschaftlichen Teiler der Zahlen dm'^2, $d'm^2$; mithin ist der vierten Folgerung im vorhergehenden Artikel zufolge F aus f und f' zusammengesetzt. — Endlich ist leicht ersichtlich, dass F aus f, f' derartig zusammengesetzt ist, wie vorgeschrieben ist, da die Zeichen der Grössen n, n' schon von Anfang an richtig bestimmt sind.

237.

Satz: Wenn die Form F in das Product zweier Formen f, f' transformierbar ist und die Form f' die Form f'' enthält, so wird F auch in das Product der Formen f, f'' transformierbar sein.

Beweis. Man behalte für die Formen F, f, f' sämtliche Bezeichnungen des Artikels 235 bei; die Form f'' sei gleich (a'', b'', c''), und es gehe f' in f'' über durch die Substitution $\alpha, \beta, \gamma, \delta$.

Dann sieht man ohne Mühe, dass F in ff'' übergeht durch die Substitution

$$\alpha p + \gamma p', \quad \beta p + \delta p', \quad \alpha p'' + \gamma p''', \quad \beta p'' + \delta p'''$$
$$\alpha q + \gamma q', \quad \beta q + \delta q', \quad \alpha q'' + \gamma q''', \quad \beta q'' + \delta q'''. \quad \text{W. z. b. w.}$$

Setzt man der Kürze wegen die Coefficienten

$$\alpha p + \gamma p', \ \beta p + \delta p', \ldots = \mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''; \ \mathfrak{Q}, \mathfrak{Q}', \mathfrak{Q}'', \mathfrak{Q}''' \text{ respective}$$

und die Zahl $\alpha\delta - \beta\gamma = e$, so bestätigt man aus den Gleichungen Ω des Artikels 235 leicht die Gleichungen:

$$
\begin{aligned}
\mathfrak{P}\mathfrak{Q}' - \mathfrak{Q}\mathfrak{P}' &= an'e\\
\mathfrak{P}\mathfrak{Q}''' - \mathfrak{Q}\mathfrak{P}''' - \mathfrak{P}'\mathfrak{Q}'' + \mathfrak{Q}'\mathfrak{P}'' &= 2bn'e\\
\mathfrak{P}''\mathfrak{Q}''' - \mathfrak{Q}''\mathfrak{P}''' &= cn'e\\
\mathfrak{P}\mathfrak{Q}'' - \mathfrak{Q}\mathfrak{P}'' = \alpha^2 a'n + 2\alpha\gamma b'n + \gamma^2 c'n &= a''n\\
\mathfrak{P}\mathfrak{Q}''' - \mathfrak{Q}\mathfrak{P}''' + \mathfrak{P}'\mathfrak{Q}'' - \mathfrak{Q}'\mathfrak{P}'' &= 2b''n\\
\mathfrak{P}'\mathfrak{Q}''' - \mathfrak{Q}'\mathfrak{P}''' &= c''n\\
\mathfrak{Q}'\mathfrak{Q}'' - \mathfrak{Q}\mathfrak{Q}''' &= Ann'e\\
\mathfrak{P}\mathfrak{Q}''' + \mathfrak{Q}\mathfrak{P}''' - \mathfrak{P}'\mathfrak{Q}'' - \mathfrak{Q}'\mathfrak{P}'' &= 2Bnn'e\\
\mathfrak{P}'\mathfrak{P}'' - \mathfrak{P}\mathfrak{P}''' &= Cnn'e.
\end{aligned}
$$

Wird jetzt die Determinante der Form f'' mit d'' bezeichnet, so ist e die Quadratwurzel aus $\frac{d''}{d'}$ und zwar die positive oder negative, je nachdem die Form f' die Form f'' eigentlich oder uneigentlich enthält. Daher ist $n'e$ die Quadratwurzel aus $\frac{d''}{D}$, woraus hervorgeht, dass die neun vorstehenden Gleichungen den Gleichungen Ω des Artikels 235 vollständig analog sind, und dass die Form f bei der Transformation der Form F in ff'' in derselben Weise genommen wird, wie bei der Transformation der Form F in ff', die Form f'' dagegen in jener entweder auf dieselbe oder auf entgegengesetzte Weise wie f' in dieser, je nachdem f' die Form f'' eigentlich oder uneigentlich enthält.

238.

Satz. Wenn die Form F unter der Form F' enthalten und in das Product der Formen f, f' transformierbar ist, so ist auch die Form F' in dasselbe Product transformierbar.

Beweis. Behält man für die Formen F, f, f' dieselben Bezeichnungen bei wie oben und nimmt man an, dass die Form F' durch die Substitution $\alpha, \beta, \gamma, \delta$ in F übergehe, so sieht man leicht, dass F' durch die Substitution

$$
\begin{array}{llll}
\alpha p + \beta q, & \alpha p' + \beta q', & \alpha p'' + \beta q'', & \alpha p''' + \beta q''',\\
\gamma p + \delta q, & \gamma p' + \delta q', & \gamma p'' + \delta q'', & \gamma p''' + \delta q'''
\end{array}
$$

ebendasselbe wird, wie F durch die Substitution $p, p', p'', p'''; q, q', q'', q'''$, und dass somit F' durch jene Substitution übergeht in ff'.

Ausserdem bestätigt man durch eine ähnliche Rechnung wie im vorigen Artikel leicht, dass F' in derselben Weise wie F in ff' transformierbar ist, wenn F' die Form F eigentlich enthält, dass dagegen, wenn F uneigentlich unter F' enthalten ist, die Transformationen der Form F in ff' und der Form F' in ff' entgegengesetzt sind in Bezug auf jede der beiden Formen f, f', dass nämlich diejenige von diesen Formen, welche in die eine Transformation direct eingeht, in der andern invers genommen wird.

Durch Combination des gegenwärtigen Satzes mit dem Satze des vorigen Artikels erhalten wir den folgenden allgemeineren **Satz:** Wenn die Form F in das Product ff' transformierbar ist und die Formen f, f' respective die Formen g, g' enthalten, die Form F aber

unter der Form G enthalten ist, so ist G in das Product gg' transformierbar. Denn nach dem Satze dieses Artikels ist G in ff', demnach nach dem Satze des vorigen Artikels in fg' und nach demselben Satze auch in gg' transformierbar. Ferner ist klar, dass, wenn alle drei Formen f, f', G die Formen g, g', F eigentlich enthalten, G auf dieselbe Weise hinsichtlich der Formen g, g' in gg' transformierbar ist, wie F hinsichtlich der Formen f, f' in ff'; dass dasselbe der Fall ist, wenn jene ersten drei Formen die letzten drei uneigentlich enthalten; endlich wird man ebenso leicht bestimmen können, auf welche Weise G in gg' transformierbar ist, wenn von den drei Formen f, f', G die eine die entsprechende Form aus den drei Formen g, g', F in anderer Weise enthält, als die beiden andern die entsprechenden Formen enthalten.

Wenn die Formen F, f, f' den Formen G, g, g' äquivalent sind, so werden diese dieselben Determinanten haben wie jene, und was die Zahlen m, m' für die Formen f, f' sind, werden sie auch für die Formen g, g' sein (Artikel 161). Hieraus leitet man mit Hülfe der vierten Folgerung des Artikels 235 ohne Schwierigkeit ab, dass in diesem Falle G aus g, g' zusammengesetzt ist, wenn F aus f, f' zusammengesetzt ist, und dass die Form g in jene Composition in derselben Weise eingeht, wie f in diese, wenn F der Form G in derselben Weise äquivalent ist, wie f der Form g und umgekehrt; und dass in ähnlicher Weise g' in der ersteren Composition entweder in derselben oder in der entgegengesetzten Weise genommen wird wie f' in der letzteren, je nachdem die Äquivalenz der Formen f', g' der Äquivalenz der Formen F, G gleichartig oder ungleichartig ist.

239.

Satz. Wenn die Form F aus den Formen f, f' zusammengesetzt ist, so wird jede andere Form, welche in das Product ff' in derselben Weise transformierbar ist, wie F, die Form F eigentlich enthalten.

Beweis. Behält man für F, f, f' sämtliche Bezeichnungen des Artikels 235 bei, so werden die Gleichungen Ω auch hier stattfinden. Nehmen wir an, dass die Form $F' = (A', B', C')$, deren Determinante gleich D' sei, in das Product ff' durch die Substitution $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \mathfrak{p}'''; \mathfrak{q}, \mathfrak{q}', \mathfrak{q}'', \mathfrak{q}'''$ übergehe, und bezeichnen wir die Zahlen

$\mathfrak{p}\mathfrak{q}' - \mathfrak{q}\mathfrak{p}', \mathfrak{p}\mathfrak{q}'' - \mathfrak{q}\mathfrak{p}'', \mathfrak{p}\mathfrak{q}''' - \mathfrak{q}\mathfrak{p}''', \mathfrak{p}'\mathfrak{q}'' - \mathfrak{q}'\mathfrak{p}'', \mathfrak{p}'\mathfrak{q}''' - \mathfrak{q}'\mathfrak{p}''', \mathfrak{p}''\mathfrak{q}''' - \mathfrak{q}''\mathfrak{p}'''$

respective mit

$$P', Q', R', S', T', U',$$

so wird man neun den Gleichungen Ω durchaus analoge Gleichungen erhalten, nämlich:

$$P' = a\mathfrak{n}', \quad R' - S' = 2b\mathfrak{n}', \quad U' = c\mathfrak{n}'$$
$$Q' = a'\mathfrak{n}, \quad R' + S' = 2b'\mathfrak{n}, \quad T' = c'\mathfrak{n}$$
$$\mathfrak{q}'\mathfrak{q}'' - \mathfrak{q}\mathfrak{q}''' = A'\mathfrak{n}\mathfrak{n}', \quad \mathfrak{p}\mathfrak{q}''' + \mathfrak{q}\mathfrak{p}''' - \mathfrak{p}'\mathfrak{q}'' - \mathfrak{q}'\mathfrak{p}'' = 2B'\mathfrak{n}\mathfrak{n}', \quad \mathfrak{p}'\mathfrak{p}'' - \mathfrak{p}\mathfrak{p}''' = C'\mathfrak{n}\mathfrak{n}',$$

die wir mit Ω' bezeichnen wollen. Die Grössen $\mathfrak{n}$, $\mathfrak{n}'$ sind hier die Quadrat-

wurzeln aus $\frac{d}{D'}$, $\frac{d'}{D'}$ und zwar mit denselben Vorzeichen genommen, wie n, n'; wenn daher die Quadratwurzel aus $\frac{D}{D'}$ (welche eine ganze Zahl ist) positiv genommen gleich k gesetzt wird, so ist $\mathfrak{n} = kn$, $\mathfrak{n}' = kn'$. Hiernach und den sechs ersten Gleichungen in Ω und Ω' zufolge ist offenbar:

$$P' = kP, \quad Q' = kQ, \quad R' = kR$$
$$S' = kS, \quad T' = kT, \quad U' = kU.$$

Daher kann man nach dem Hülfssatz im Artikel 234 vier ganze Zahlen α, β, γ, δ, von solcher Beschaffenheit bestimmen, dass

$$\alpha p + \beta q = \mathfrak{p}, \quad \gamma p + \delta q = \mathfrak{q}$$
$$\alpha p' + \beta q' = \mathfrak{p}', \quad \gamma p' + \delta q' = \mathfrak{q}'$$
u. s. w.

und

$$\alpha\delta - \beta\gamma = k$$

wird. Substituiert man diese Werte von $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{p}'$, $\mathfrak{q}'$, ... in die letzten drei Gleichungen von Ω', so bestätigt man leicht mit Hülfe der Gleichungen $\mathfrak{n} = kn$, $\mathfrak{n}' = kn'$ und der drei letzten Gleichungen von Ω die Gleichungen:

$$A'\alpha^2 + 2B'\alpha\gamma + C'\gamma^2 = A$$
$$A'\alpha\beta + B'(\alpha\delta + \beta\gamma) + C'\gamma\delta = B$$
$$A'\beta^2 + 2B'\beta\delta + C'\delta^2 = C.$$

Es geht daher die Form F' durch die Substitution α, β, γ, δ (welche eine eigentliche ist, da $\alpha\delta - \beta\gamma = k$ positiv ist) in F über, d. h. sie enthält die Form F eigentlich. W. z. b. w.

Wenn daher die Form F' aus den Formen f, f' ebenfalls zusammengesetzt ist (in derselben Weise wie F aus ihnen), so werden die Formen F, F' dieselbe Determinante haben und daher eigentlich äquivalent sein. Allgemeiner: Wenn die Form G aus den Formen g, g' in derselben Weise zusammengesetzt ist, wie F aus f, f' respective, und die Formen g, g' den Formen f, f' eigentlich äquivalent sind, so werden auch die Formen F, G eigentlich äquivalent sein.

Da derjenige Fall, in welchem die beiden zu componierenden Formen in die Composition direct eingehen, der einfachste ist und auf ihn die übrigen leicht zurückgeführt werden können, so werden wir im Folgenden nur jenen betrachten, so dass, wenn irgend eine Form aus zwei andern zusammengesetzt genannt wird, darunter immer zu verstehen ist, dass jene aus jeder der beiden Formen eigentlich zusammengesetzt ist.*) Die-

*) Analog wird bei der Zusammensetzung der Verhältnisse (welche mit der Zusammensetzung der Formen grosse Ähnlichkeit hat) gewöhnlich stillschweigend angenommen, dass die zu componierenden Verhältnisse direct genommen werden sollen, falls nicht das Gegenteil gesagt wird.

selbe Einschränkung wird gelten, wenn eine Form in das Product zweier andern transformierbar genannt wird.

240.

Satz. Wenn aus den Formen f, f' die Form F, aus F, f'' die Form $\mathfrak{F}$, aus f, f'' die Form F' und aus F', f' die Form $\mathfrak{F}'$ zusammengesetzt ist, so sind die Formen $\mathfrak{F}$, $\mathfrak{F}'$ eigentlich äquivalent.

Beweis. I. Es sei

$$\begin{aligned} f &= ax^2 + 2bxy + cy^2 \\ f' &= a'x'^2 + 2b'x'y' + c'y'^2 \\ f'' &= a''x''^2 + 2b''x''y'' + c''y''^2 \\ F &= AX^2 + 2BXY + CY^2 \\ F' &= A'X'^2 + 2B'X'Y' + C'Y'^2 \\ \mathfrak{F} &= \mathfrak{A}\mathfrak{X}^2 + 2\mathfrak{B}\mathfrak{X}\mathfrak{Y} + \mathfrak{C}\mathfrak{Y}^2 \\ \mathfrak{F}' &= \mathfrak{A}'\mathfrak{X}'^2 + 2\mathfrak{B}'\mathfrak{X}'\mathfrak{Y}' + \mathfrak{C}'\mathfrak{Y}'^2, \end{aligned}$$

ferner seien die Determinanten dieser sieben Formen resp. d, d', d'', D, D', $\mathfrak{D}$, $\mathfrak{D}'$; diese werden sämtlich dasselbe Vorzeichen haben und in dem Verhältnis von Quadratzahlen zu einander stehen. Weiter sei m der grösste gemeinschaftliche Teiler der Zahlen a, $2b$, c und eine analoge Bedeutung mögen m', m'', M hinsichtlich der Formen f', f'', F haben. Dann ist der vierten Folgerung im Artikel 235 gemäss D der grösste gemeinschaftliche Teiler der Zahlen dm'^2, $d'm^2$ und demnach Dm''^2 der grösste gemeinschaftliche Teiler der Zahlen $dm'^2m''^2$, $d'm^2m''^2$; $M = mm'$; $\mathfrak{D}$ der grösste gemeinschaftliche Teiler der Zahlen Dm''^2, $d''M^2$ oder der Zahlen Dm''^2, $d''m^2m'^2$. Hieraus folgt, dass $\mathfrak{D}$ der grösste gemeinschaftliche Teiler der drei Zahlen $dm'^2m''^2$, $d'm^2m''^2$, $d''m^2m'^2$ ist. Aus analogem Grunde ist aber $\mathfrak{D}'$ der grösste gemeinschaftliche Teiler ebenderselben drei Zahlen; demnach ist, weil $\mathfrak{D}$ und $\mathfrak{D}'$ dasselbe Zeichen haben, $\mathfrak{D} = \mathfrak{D}'$, oder die beiden Formen $\mathfrak{F}$, $\mathfrak{F}'$ haben dieselbe Determinante.

II. Es möge nun F in ff' durch die Substitution

$$\begin{aligned} X &= pxx' + p'xy' + p''yx' + p'''yy' \\ Y &= qxx' + q'xy' + q''yx' + q'''yy' \end{aligned}$$

und $\mathfrak{F}$ in Ff'' durch die Substitution

$$\begin{aligned} \mathfrak{X} &= \mathfrak{p}Xx'' + \mathfrak{p}'Xy'' + \mathfrak{p}''Yx'' + \mathfrak{p}'''Yy'' \\ \mathfrak{Y} &= \mathfrak{q}Xx'' + \mathfrak{q}'Xy'' + \mathfrak{q}''Yx'' + \mathfrak{q}'''Yy'' \end{aligned}$$

übergehen, und es mögen die positiven Quadratwurzeln aus $\frac{d}{D}$, $\frac{d'}{D}$, $\frac{D}{\mathfrak{D}}$, $\frac{d''}{\mathfrak{D}}$ mit n, n', $\mathfrak{N}$, $\mathfrak{n}''$ bezeichnet werden. Dann hat man nach Artikel 235

achtzehn Gleichungen, von denen die eine Hälfte zur Transformation der Form F in ff', die andere zur Transformation der Form $\mathfrak{F}$ in Ff'' gehört. Die erste ist $pq' - qp' = an'$ und nach deren Muster können die übrigen, die wir der Kürze wegen hier weglassen müssen, leicht gebildet werden. Übrigens werden die Grössen n, n', $\mathfrak{N}$, $\mathfrak{n}''$ zwar rationale, aber nicht notwendig ganze Zahlen sein.

III. Wenn die Werte von X, Y in die Werte von $\mathfrak{X}$, $\mathfrak{Y}$ substituiert werden, so ergiebt sich folgende Substitution:

$$\begin{aligned} \mathfrak{X} = &\ (1)xx'x'' + (2)xx'y'' + (3)xy'x'' + (4)xy'y'' \\ &+ (5)yx'x'' + (6)yx'y'' + (7)yy'x'' + (8)yy'y'' \\ \mathfrak{Y} = &\ (9)xx'x'' + (10)xx'y'' + (11)xy'x'' + (12)xy'y'' \\ &+ (13)yx'x'' + (14)yx'y'' + (15)yy'x'' + (16)yy'y'', \end{aligned}$$

durch welche offenbar $\mathfrak{F}$ in das Product $ff'f''$ übergeht. Der Coefficient (1) ist gleich $p\mathfrak{p} + q\mathfrak{p}''$; die Werte der fünfzehn übrigen setzen wir nicht hierher, weil sie jeder ohne Schwierigkeit entwickeln kann. Die Zahl $(1)(10) - (2)(9)$ werden wir mit $(1, 2)$, die Zahl $(1)(11) - (3)(9)$ mit $(1, 3)$ und allgemein $(g)(8+h) - (h)(8+g)$ mit (g, h) bezeichnen, indem wir annehmen, dass g, h verschiedene ganze Zahlen zwischen 1 und 16, deren grössere h ist, seien.*) Auf diese Weise erhält man im Ganzen achtundzwanzig Zeichen. Bezeichnet man nun die positiven Quadratwurzeln aus $\frac{d}{\mathfrak{D}}$, $\frac{d'}{\mathfrak{D}}$ mit $\mathfrak{n}$, $\mathfrak{n}'$ (welche gleich $n\mathfrak{N}$, $n'\mathfrak{N}$ sein werden), so findet man die folgenden achtundzwanzig Gleichungen:

$(1, 2) = aa'\mathfrak{n}''$	$(3, 5) = a''b'\mathfrak{n} - a''b\mathfrak{n}'$
$(1, 3) = aa''\mathfrak{n}'$	$(3, 6) = bb'\mathfrak{n}'' + b'b''\mathfrak{n} - bb''\mathfrak{n}' - \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}''$
$(1, 4) = ab'\mathfrak{n}'' + ab''\mathfrak{n}'$	$(3, 7) = a''c'\mathfrak{n}$
$(1, 5) = a'a''\mathfrak{n}$	$(3, 8) = bc'\mathfrak{n}'' + b''c'\mathfrak{n}$
$(1, 6) = a'b\mathfrak{n}'' + a'b''\mathfrak{n}$	$(4, 5) = b'b''\mathfrak{n} - bb'\mathfrak{n}'' - bb''\mathfrak{n}' + \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}''$
$(1, 7) = a''b\mathfrak{n}' + a''b'\mathfrak{n}$	$(4, 6) = b'c''\mathfrak{n} - bc''\mathfrak{n}'$
$(1, 8) = bb'\mathfrak{n}'' + bb''\mathfrak{n}' + b'b''\mathfrak{n} + \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}''$	$(4, 7) = b''c'\mathfrak{n} - bc'\mathfrak{n}''$
$(2, 3) = ab''\mathfrak{n}' - ab'\mathfrak{n}''$	$(4, 8) = c'c''\mathfrak{n}$
$(2, 4) = ac''\mathfrak{n}'$	$(5, 6) = ca'\mathfrak{n}''$
$(2, 5) = a'b''\mathfrak{n} - a'b\mathfrak{n}''$	$(5, 7) = ca''\mathfrak{n}'$
$(2, 6) = a'c''\mathfrak{n}$	$(5, 8) = b'c\mathfrak{n}'' + b''c\mathfrak{n}'$
$(2, 7) = bb''\mathfrak{n}' + b'b''\mathfrak{n} - bb'\mathfrak{n}'' - \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}''$	$(6, 7) = b''c\mathfrak{n}' - b'c\mathfrak{n}''$
$(2, 8) = bc''\mathfrak{n}' + b'c''\mathfrak{n}$	$(6, 8) = cc''\mathfrak{n}'$
$(3, 4) = ac'\mathfrak{n}''$	$(7, 8) = cc'\mathfrak{n}''$,

*) Die gegenwärtige Bedeutung dieser Zeichen ist nicht zu verwechseln mit derjenigen, in welcher sie im Artikel 234 genommen waren; denn die hier durch diese Zeichen ausgedrückten Zahlen entsprechen gerade denjenigen, welche im Artikel 234 mit den dort durch ähnliche Zeichen bezeichneten Zahlen multipliciert sind.

welche wir mit Φ bezeichnen wollen, und neun andere:

$$\begin{array}{rl}
(10)(11)-(\ 9)(12) & = a\mathfrak{n}'\mathfrak{n}''\mathfrak{A} \\
(1)(12)-(\ 2)(11)-(\ 3)(10)+(\ 4)(\ 9) & = 2a\mathfrak{n}'\mathfrak{n}''\mathfrak{B} \\
(\ 2)(\ 3)-(\ 1)(\ 4) & = a\mathfrak{n}'\mathfrak{n}''\mathfrak{C} \\
-(9)(16)+(10)(15)+(11)(14)-(12)(13) & = 2b\mathfrak{n}'\mathfrak{n}''\mathfrak{A} \\
\left.\begin{array}{r}(1)(16)-(\ 2)(15)-(\ 3)(14)+(\ 4)(13) \\ +(5)(12)-(\ 6)(11)-(\ 7)(10)+(\ 8)(\ 9)\end{array}\right\} & = 4b\mathfrak{n}'\mathfrak{n}''\mathfrak{B} \\
-(1)(\ 8)+(\ 2)(\ 7)+(\ 3)(\ 6)-(\ 4)(\ 5) & = 2b\mathfrak{n}'\mathfrak{n}''\mathfrak{C} \\
(14)(15)-(13)(16) & = c\mathfrak{n}'\mathfrak{n}''\mathfrak{A} \\
(5)(16)-(\ 6)(15)-(\ 7)(14)+(\ 8)(13) & = 2c\mathfrak{n}'\mathfrak{n}''\mathfrak{B} \\
(\ 6)(\ 7)-(\ 5)(\ 8) & = c\mathfrak{n}'\mathfrak{n}''\mathfrak{C}',
\end{array}$$

die wir mit Ψ bezeichnen werden.*)

IV. Die Ableitung aller dieser 37 Gleichungen anzugeben, würde allzu weitläufig sein; es wird genügen, einige zu bestätigen, nach deren Muster die übrigen ohne Schwierigkeit bewiesen werden können.

1. Man hat:

$$\begin{aligned}
(1, 2) &= (1)(10)-(2)(9) \\
&= (\mathfrak{p}\mathfrak{q}'-\mathfrak{q}\mathfrak{p}')p^2+(\mathfrak{p}\mathfrak{q}'''-\mathfrak{q}\mathfrak{p}'''-\mathfrak{p}'\mathfrak{q}''+\mathfrak{q}'\mathfrak{p}'')pq+(\mathfrak{p}''\mathfrak{q}'''-\mathfrak{q}''\mathfrak{p}''')q^2 \\
&= \mathfrak{n}''(Ap^2+2Bpq+Cq^2) = \mathfrak{n}''aa',
\end{aligned}$$

und dieses ist die erste Gleichung.

2. Es ist:

$$(1, 3) = (1)(11)-(3)(9) = (\mathfrak{p}\mathfrak{q}''-\mathfrak{q}\mathfrak{p}'')(pq'-qp') = a''\mathfrak{N}an' = aa''\mathfrak{n}',$$

und dieses ist die zweite Gleichung.

3. Es ist:

$$\begin{aligned}
(1, 8) &= (1)(16)-(8)(9) \\
&= (\mathfrak{p}\mathfrak{q}'-\mathfrak{q}\mathfrak{p}')pp'''+(\mathfrak{p}\mathfrak{q}'''-\mathfrak{q}\mathfrak{p}''')pq'''-(\mathfrak{p}'\mathfrak{q}''-\mathfrak{q}'\mathfrak{p}'')qp''' \\
&\qquad +(\mathfrak{p}''\mathfrak{q}'''-\mathfrak{q}''\mathfrak{p}''')qq''' \\
&= \mathfrak{n}''[App'''+B(pq'''+qp''')+Cqq''']+b''\mathfrak{N}(pq'''-qp''') \\
&= \mathfrak{n}''(bb'+\sqrt{dd'})+b''\mathfrak{N}(b'n+bn')^{**)} \\
&= \mathfrak{n}''bb'+\mathfrak{n}'bb''+\mathfrak{n}b'b''+\mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}''.
\end{aligned}$$

Dies ist die achte Gleichung in Φ. Wir überlassen es dem Leser, die übrigen Gleichungen zu bestätigen.

V. Aus den Gleichungen Φ ergiebt sich in folgender Weise, dass die achtundzwanzig Zahlen $(1, 2)$, $(1, 3)$, ... keinen gemeinschaftlichen Teiler

---

*) Es möge bemerkt werden, dass man 18 andere diesen Gleichungen Ψ ähnliche erhalten kann, in denen rechts an Stelle der Factoren a, $2b$, c resp. a', $2b'$, c'; a'', $2b''$, c'' stehen; da diese aber für unsern Zweck nicht notwendig sind, lassen wir sie weg.

**) Dies folgt aus Gl. 10 des Art. 235 u. ff. Die Wurzelgrösse $\sqrt{dd'}$ ist gleich $Dnn' = \mathfrak{D}nn'\mathfrak{N}^2 = \mathfrak{D}\mathfrak{n}\mathfrak{n}'$.

haben: Wir bemerken zunächst, dass die siebenundzwanzig Producte aus drei Factoren, von denen entweder der erste $\mathfrak{n}$, der zweite irgend eine der Zahlen a', $2b'$, c', der dritte irgend eine der Zahlen a'', $2b''$, c'', oder der erste $\mathfrak{n}'$, der zweite irgend eine der Zahlen a, $2b$, c, der dritte irgend eine der Zahlen a'', $2b''$, c'', oder endlich der erste $\mathfrak{n}''$, der zweite irgend eine der Zahlen a, $2b$, c, der dritte irgend eine der Zahlen a', $2b'$, c' ist — dass diese einzelnen siebenundzwanzig Producte den Gleichungen Φ zufolge entweder irgend einer der achtundzwanzig Zahlen $(1,2)$, $(1,3)$, ... oder der Summe oder Differenz mehrerer von ihnen gleich sind (z. B. $\mathfrak{n}a'a''=(1,5)$, $2\mathfrak{n}a'b''=(1,6)+(2,5)$, $4\mathfrak{n}b'b''=(1,8)+(2,7)+(3,6)+(4,5)$ und ähnlich bei den übrigen); wenn daher diese Zahlen einen gemeinschaftlichen Teiler hätten, so müsste dieser notwendig auch in allen jenen Producten aufgehen. Hieraus aber ergiebt sich leicht mit Hülfe des Artikels 40 und nach einem im Vorhergehenden öfter angewendeten Verfahren, dass derselbe Teiler auch in den Zahlen $\mathfrak{n}m'm''$, $\mathfrak{n}'mm''$, $\mathfrak{n}''mm'$ aufgehen muss, und daher die Quadrate dieser, welche gleich $\frac{dm'^2m''^2}{\mathfrak{D}}$, $\frac{d'm^2m''^2}{\mathfrak{D}}$, $\frac{d''m^2m'^2}{\mathfrak{D}}$ sind, durch das Quadrat desselben teilbar sind. Dies ist aber absurd, da nach I der grösste gemeinschaftliche Teiler der drei Zähler gleich $\mathfrak{D}$ ist, und daher die Quadrate selbst keinen gemeinschaftlichen Teiler haben können.

VI. Dies bezieht sich alles auf die Transformation der Form $\mathfrak{F}$ in $ff'f''$ und ist aus den Transformationen der Form F in ff' und der Form $\mathfrak{F}$ in Ff'' abgeleitet. Auf ganz ähnliche Weise aber wird aus den Transformationen der Form F' in ff'' und der Form $\mathfrak{F}'$ in $F'f'$ die folgende Transformation der Form $\mathfrak{F}'$ in $ff'f''$ hergeleitet:

$$\mathfrak{X}' = (1)'xx'x'' + (2)'xx'y'' + (3)'xy'x'' + \dots$$
$$\mathfrak{Y} = (9)'xx'x'' + (10)'xx'y'' + (11)'xy'x'' + \dots$$

(indem man sämtliche Coefffcienten in ähnlicher Weise bezeichnet wie bei der Transformation der Form $\mathfrak{F}$ in $ff'f''$ und jedem einzelnen zur Unterscheidung einen Strich anfügt), aus der sich ebenso wie vorher achtundzwanzig Φ analoge Gleichungen, die wir mit Φ' bezeichnen, und neun andere Ψ analoge Gleichungen, die wir mit Ψ' bezeichnen, ergeben. Bezeichnet man nämlich

$$(1)'(10)' - (2)'(9)' \text{ mit } (1,2)', \quad (1)'(11)' - (3)'(9)' \text{ mit } (1,3)', \text{ u. s. w.,}$$

so werden die Gleichungen Φ':

$$(1,2)' = aa'\mathfrak{n}'', \quad (1,3)' = aa''\mathfrak{n}', \dots$$

und die Gleichungen Ψ':

$$(10)'(11)' - (9)'(12)' = a\mathfrak{n}'\mathfrak{n}''\mathfrak{A}', \dots$$

(Eine weitere Entwicklung überlassen wir der Kürze wegen dem Leser; übrigens werden Kundige finden, dass diese neue Rechnung nicht einmal

nötig ist, sondern die erste Analyse durch Analogie leicht hierauf übertragen werden kann). Hiernach folgt aus Φ und Φ' sogleich:

$$(1,2)=(1,2)',\quad (1,3)=(1,3)',\quad (1,4)=(1,4)',\quad (2,3)=(2,3)',\ \ldots$$

Hieraus aber und daraus, dass (1, 2), (1, 3), (2, 3), ... (nach V) nicht sämtlich einen gemeinschaftlichen Teiler haben, ergiebt sich mit Hülfe des Hülfssatzes im Artikel 234, dass man vier ganze Zahlen α, β, γ, δ so bestimmen kann, dass

$$\alpha(1)'+\beta(9)'=(1),\quad \alpha(2)'+\beta(10)'=(2),\quad \alpha(3)'+\beta(11)'=(3),\ldots$$
$$\gamma(1)'+\delta(9)'=(9),\quad \gamma(2)'+\delta(10)'=(10),\quad \gamma(3)'+\delta(11)'=(11),\ldots$$

und $\alpha\delta-\beta\gamma=1$ ist.

VII. Hieraus und dadurch, dass man aus den ersten drei Gleichungen von Ψ die Werte von $a\mathfrak{A}$, $a\mathfrak{B}$, $a\mathfrak{C}$ und aus den ersten drei Gleichungen von Ψ' die Werte von $a\mathfrak{A}'$, $a\mathfrak{B}'$, $a\mathfrak{C}'$ substituiert, wird leicht bestätigt, dass

$$a(\mathfrak{A}\alpha^2+2\mathfrak{B}\alpha\gamma+\mathfrak{C}\gamma^2)=a\mathfrak{A}'$$
$$a\big(\mathfrak{A}\alpha\beta+\mathfrak{B}(\alpha\delta+\beta\gamma)+\mathfrak{C}\gamma\delta\big)=a\mathfrak{B}'$$
$$a(\mathfrak{A}\beta^2+2\mathfrak{B}\beta\delta+\mathfrak{C}\delta^2)=a\mathfrak{C}'$$

ist, woraus offenbar, falls nicht $a=0$ ist, folgt, dass die Form $\mathfrak{F}$ durch die eigentliche Substitution α, β, γ, δ in $\mathfrak{F}'$ übergeht. — Wendet man aber statt der drei ersten Gleichungen in Ψ und Ψ' die drei folgenden an, so findet man drei den eben angegebenen völlig analoge Gleichungen, in denen an Stelle des Factors a überall b steht, woraus hervorgeht, dass derselbe Schluss gilt, wofern nur nicht $b=0$ ist. Wendet man schliesslich die drei letzten Gleichungen in Ψ und Ψ' an, so findet man auf dieselbe Weise, dass unser Schluss richtig ist, wofern nur nicht $c=0$ ist. Da nun sicher nicht alle drei Grössen a, b, c gleichzeitig gleich 0 sind, so muss notwendig die Form $\mathfrak{F}$ durch die Substitution α, β, γ, δ übergehen in $\mathfrak{F}'$, und demnach wird sie dieser Form eigentlich äquivalent sein. W. z. b. w.

241.

Eine solche Form wie $\mathfrak{F}$ oder $\mathfrak{F}'$, welche entsteht, wenn die eine von drei gegebenen Formen mit derjenigen, welche aus der Composition der beiden übrigen sich ergiebt, zusammengesetzt wird, werden wir aus diesen drei Formen zusammengesetzt nennen, und aus dem vorigen Artikel geht hervor, dass es gleichgültig ist, in welcher Reihenfolge die drei Formen componiert werden. Analog, wenn beliebig viele Formen f, f', f'', f''', ... (deren Determinanten im quadratischen Verhältnis zu einander stehen müssen) gegeben sind, und es wird die Form f mit f' componiert, die daraus sich ergebende mit f'', die hierdurch entstehende mit f''' u. s. w., so wird die Form, welche am Schlusse dieser Operation sich ergiebt, aus allen Formen f, f', f'', f''', ... zusammengesetzt genannt werden. Man beweist leicht, dass es auch hierbei gleichgiltig ist, in welcher Reihenfolge die Formen zusammengesetzt werden, d. h. in

welcher Reihenfolge auch diese Formen zusammengesetzt werden mögen, es werden stets die aus dieser Zusammensetzung hervorgehenden Formen eigentlich äquivalent sein. — Ferner ist klar, dass, wenn den Formen f, f', f'', ... die Formen g, g', g'', ... eigentlich äquivalent sind, auch die aus diesen zusammengesetzte Form der aus jenen zusammengesetzten Form eigentlich äquivalent sein wird.

242.

Die vorstehenden Sätze beziehen sich auf die Composition der Formen in ihrer grössten Allgemeinheit; wir gehen jetzt zu **specielleren Anwendungen** über, durch welche wir die Reihe jener nicht unterbrechen wollten. Zunächst nehmen wir die Aufgabe des Artikels 236 wieder auf, die wir durch folgende Bedingungen beschränken: Erstens sollen die zu componierenden Formen dieselbe Determinante haben, also $d = d'$ sein; zweitens sollen m, m' prim zu einander sein; drittens soll die gesuchte Form direct aus jeder der beiden Formen f, f' zusammengesetzt sein. Hiernach werden auch m^2 und m'^2 zu einander prim sein, und daher ist der grösste gemeinschaftliche Teiler der Zahlen dm'^2, $d'm^2$, d. h. $D = d = d'$ und $n = n' = 1$. Die vier Grössen $\mathfrak{Q}$, $\mathfrak{Q}'$, $\mathfrak{Q}''$, $\mathfrak{Q}'''$, die nach Belieben angenommen werden können, werden wir respective gleich -1, 0, 0, 0 setzen, was immer erlaubt ist, ausser in dem einzigen Falle, wo a, a', $b + b'$ gleichzeitig gleich 0 sind, auf den wir daher hier keine Rücksicht nehmen; offenbar aber kann dieser Fall nur eintreten bei Formen mit positiver quadratischer Determinante. Dann ist klar, dass μ der grösste gemeinschaftliche Teiler der Zahlen a, a', $b + b'$ ist, dass die Zahlen $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ derart angenommen werden müssen, dass

$$\mathfrak{P}'a + \mathfrak{P}''a' + \mathfrak{P}'''(b + b') = \mu$$

wird, dass aber $\mathfrak{P}$ völlig willkürlich ist. Hieraus ergiebt sich, wenn man am angeführten Orte für p, q, p' q', ... ihre Werte substituiert:

$$A = \frac{aa'}{\mu^2}, \quad B = \frac{1}{\mu}\,[\mathfrak{P}aa' + \mathfrak{P}'ab' + \mathfrak{P}''a'b + \mathfrak{P}'''(bb' + D)];$$

C aber kann durch die Gleichung $AC = B^2 - D$ bestimmt werden, wofern nicht a und a' gleichzeitig gleich 0 sind.

In dieser Lösung hängt demnach der Wert von A nicht von den Werten $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ (welche auf unendlich viele verschiedene Arten bestimmt werden können) ab; B jedoch wird andere Werte erhalten, wenn man diesen Zahlen andere Werte beilegt, und es verlohnt sich zu untersuchen, auf welche Weise sämtliche Werte von B unter sich zusammenhängen. Zu diesem Zwecke bemerken wir:

I. Wie auch immer die Zahlen $\mathfrak{P}$. $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ bestimmt werden mögen, die daraus hervorgehenden Werte von B sind sämtlich nach dem Modul A congruent. Nehmen wir an, dass, wenn

$$\mathfrak{P} = \mathfrak{p}, \quad \mathfrak{P}' = \mathfrak{p}', \quad \mathfrak{P}'' = \mathfrak{p}'', \quad \mathfrak{P}''' = \mathfrak{p}''' \text{ gesetzt wird, } B = \mathfrak{B} \text{ ist,}$$

wenn aber

$\mathfrak{P} = \mathfrak{p} + \mathfrak{d}$, $\mathfrak{P}' = \mathfrak{p}' + \mathfrak{d}'$, $\mathfrak{P}'' = \mathfrak{p}'' + \mathfrak{d}''$, $\mathfrak{P}''' = \mathfrak{p}''' + \mathfrak{d}'''$ gesetzt wird, $B = \mathfrak{B} + \mathfrak{D}$ werde, so ist:

$$a\mathfrak{d}' + a'\mathfrak{d}'' + (b+b')\,\mathfrak{d}''' = 0, \quad aa'\mathfrak{d} + ab'\mathfrak{d}' + a'b\mathfrak{d}'' + (bb' + D)\,\mathfrak{d}''' = \mu\mathfrak{D}.$$

Multipliciert man die linke Seite der zweiten Gleichung mit $a\mathfrak{p}' + a'\mathfrak{p}'' + (b+b')\,\mathfrak{p}'''$, die rechte mit μ und subtrahiert von dem ersten Producte die Grösse

$$(ab'\mathfrak{p}' + a'b\mathfrak{p}'' + (b'^2 + D)\,\mathfrak{p}''')\,(a\mathfrak{d}' + a'\mathfrak{d}'' + (b+b')\,\mathfrak{d}'''),$$

welche der ersten Gleichung zufolge offenbar gleich 0 ist, so erhält man, nachdem man entwickelt und, was sich hebt, weggelassen hat:

$$aa'\big[\mu\mathfrak{d} + \big((b'-b)\,\mathfrak{p}'' + c'\mathfrak{p}'''\big)\mathfrak{d}' + \big((b-b')\,\mathfrak{p}' + c\mathfrak{p}'''\big)\,\mathfrak{d}'' - \big(c'\mathfrak{p}' + c\mathfrak{p}''\big)\,\mathfrak{d}'''\big] = \mu^2\mathfrak{D},$$

wonach offenbar $\mu^2\mathfrak{D}$ durch aa' oder $\mathfrak{D}$ durch $\frac{aa'}{\mu^2}$ d. h. durch A teilbar und

$$\mathfrak{B} \equiv (\mathfrak{B} + \mathfrak{D}) \pmod{\mathfrak{A}}$$

ist.

II. Wenn für die Werte $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \mathfrak{p}'''$ von $\mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''$: $B = \mathfrak{B}$ wird, so lassen sich andere Werte dieser Zahlen finden, infolge deren B irgend einen gegebenen, $\mathfrak{B}$ nach dem Modul A congruenten Wert, etwa den Wert $\mathfrak{B} + kA$, erhält. Zunächst bemerken wir, dass die vier Zahlen μ, c, c', $b - b'$ keinen gemeinschaftlichen Teiler haben können; denn wenn sie einen solchen hätten, so würde dieser in den sechs Zahlen a, a', $b + b'$, c, c', $b - b'$ und daher auch sowohl in a, $2b$, c, als auch in a', $2b'$, c', und folglich auch in m, m' aufgehen, die aber nach Voraussetzung prim zu einander sind. Daher lassen sich vier ganze Zahlen h, h', h'', h''' von der Beschaffenheit angeben, dass

$$h\mu + h'c + h''c' + h'''(b - b') = 1$$

wird. Ist dies geschehen und setzt man:

$$kh = \mathfrak{d}, \qquad k[h''(b+b') - h'''a'] = \mu\mathfrak{d}'$$
$$k[h'(b+b') + h'''a] = \mu\mathfrak{d}'', \qquad -k(h'a' + h''a) = \mu\mathfrak{d}''',$$

so sind offenbar $\mathfrak{d}, \mathfrak{d}', \mathfrak{d}'', \mathfrak{d}'''$ ganze Zahlen; ferner bestätigt man leicht, dass

$$a\mathfrak{d}' + a'\mathfrak{d}'' + (b+b')\,\mathfrak{d}''' = 0$$

$$aa'\mathfrak{d} + ab'\mathfrak{d}' + a'b\mathfrak{d}'' + (bb' + D)\,\mathfrak{d}''' = \frac{aa'k}{\mu}[\mu h + ch' + c'h'' + (b-b')\,h''' = \mu kA$$

ist. Aus der ersten Gleichung geht hervor, dass auch $\mathfrak{p} + \mathfrak{d}$, $\mathfrak{p}' + \mathfrak{d}'$, $\mathfrak{p}'' + \mathfrak{d}''$, $\mathfrak{p}''' + \mathfrak{d}'''$ Werte von $\mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''$ sind, aus der letzten, dass diese Werte $B = \mathfrak{B} + kA$ ergeben.

Hieraus erhellt, dass B immer so bestimmt werden kann, dass es zwischen 0 und $A-1$ incl., wenn A positiv ist, und zwischen 0 und $-A-1$, wenn A negativ ist, liegt.

243.

Aus den Gleichungen

$$\mathfrak{P}'a+\mathfrak{P}''a'+\mathfrak{P}'''(b+b')=\mu,\quad B=\frac{1}{\mu}[\mathfrak{P}aa'+\mathfrak{P}'ab'+\mathfrak{P}''a'b+\mathfrak{P}'''(bb'+D)]$$

folgt:

$$B=b+\frac{a}{\mu}[\mathfrak{P}a'+\mathfrak{P}'(b'-b)-\mathfrak{P}'''c]=b'+\frac{a'}{\mu}[\mathfrak{P}a+\mathfrak{P}''(b-b')-\mathfrak{P}'''c'],$$

daher

$$B\equiv b\left(\text{mod.}\,\frac{a}{\mu}\right)\text{ und }B\equiv b'\left(\text{mod.}\,\frac{a'}{\mu}\right).$$

So oft $\frac{a}{\mu}$, $\frac{a'}{\mu}$ prim zu einander sind, wird zwischen 0 und $A-1$ (oder zwischen 0 und $-A-1$, falls A negativ ist) nur eine einzige Zahl liegen, welche $\equiv b\left(\text{mod.}\,\frac{a}{\mu}\right)$ und $\equiv b'\left(\text{mod.}\,\frac{a'}{\mu}\right)$ ist; wird dieselbe gleich B und $\frac{B^2-D}{A}=C$ gesetzt, so ist offenbar die Form (A, B, C) aus den Formen (a, b, c), (a', b', c') zusammengesetzt. In diesem Falle braucht man sich also, um die zusammengesetzte Form zu finden, um die Zahlen $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ nicht weiter zu kümmern*).

Wenn z. B. die aus den Formen (10, 3, 11), (15, 2, 7) zusammengesetzte Form gesucht wird, so sind a, a', $b+b'$ respective gleich 10, 15, 5; $\mu=5$; hieraus $A=6$; $B\equiv 3$ (mod. 2) und $\equiv 2$ (mod. 3), somit $B=5$ und die gesuchte Form ist (6, 5, 21). — Übrigens ist die Bedingung, dass $\frac{a}{\mu}$, $\frac{a'}{\mu}$ prim zu einander seien, vollständig äquivalent der Bedingung, dass die beiden Zahlen a, a' keinen grösseren gemeinschaftlichen Teiler haben sollen, als die drei a, a', $b+b'$ oder, was auf dasselbe hinauskommt, dass der grösste gemeinschaftliche Teiler der Zahlen a, a' auch in der Zahl $b+b'$ aufgehen solle. Es mögen insbesondere die folgenden speciellen Fälle angeführt werden.

1. Sind zwei Formen (a, b, c), (a', b', c') mit derselben Determinante D von solcher Beschaffenheit gegeben, dass der grösste gemeinschaftliche Teiler der Zahlen a, $2b$, c zum grössten gemeinschaftlichen Teiler der Zahlen a', $2b'$, c' und ferner a zu a' prim ist, so findet man die aus ihnen zusammengesetzte Form (A, B, C), indem man $A=aa'$, $B\equiv b$ (mod. a) und $\equiv b'$ (mod. a'), $C=\frac{B^2-D}{A}$ setzt. Dieser Fall findet immer

*) Was immer bewirkt wird durch Anwendung der Congruenzen:

$$\frac{aB}{\mu}\equiv\frac{ab'}{\mu},\ \frac{a'B}{\mu}\equiv\frac{a'b}{\mu},\ \frac{(b+b')B}{\mu}\equiv\frac{bb'+D}{\mu}\ (\text{mod. } A).$$

statt, wenn eine der zu componierenden Formen die Hauptform, nämlich $a=1$, $b=0$, $c=-D$ ist. Dann wird $A=a'$, B kann gleich b' gesetzt werden, woraus dann $C=c'$ folgt. Mithin ist die aus der Hauptform und irgend einer andern Form mit derselben Determinante zusammengesetzte Form diese Form selbst.

2. Wenn zwei entgegengesetzte eigentlich primitive Formen zu componieren sind, etwa (a, b, c) und $(a, -b, c)$, so ist $\mu=a$. Hieraus erkennt man leicht, dass die Hauptform $(1, 0, -D)$ aus jenen zusammengesetzt ist.

3. Sind beliebig viele eigentlich primitive Formen (a, b, c), (a', b', c'), (a'', b'', c''), ... mit derselben Determinante D gegeben, deren Anfangsglieder a, a' a'', ... zu einander prime Zahlen sind, so findet man die aus jenen zusammengesetzte Form (A, B, C), wenn man A gleich dem Producte aus allen Zahlen a, a', a'', ..., B den einzelnen b, b', b'', ... nach den Moduln a, a', a'', ... respective congruent und $C=\frac{B^2-D}{A}$ setzt. Denn man sieht leicht, dass die aus zwei Formen (a, b, c), (a', b', c') zusammengesetzte Form lautet: $\left(aa', B, \frac{B^2-D}{aa'}\right)$, die aus dieser und der Form (a'', b'', c'') zusammengesetzte Form: $\left(aa'a'', B, \frac{B^2-D}{aa'a''}\right)$ u. s. w. — Umgekehrt

4. Wenn eine eigentlich primitive Form (A, B, C) mit der Determinante D gegeben ist und das Glied A in beliebig viele zu einander prime Factoren a, a', a'', ... zerlegt wird, ferner die Zahlen b, b' b'', ... entweder gleich B oder wenigstens B nach den Moduln a, a', a'' ... respective congruent angenommen werden und $ac=b^2-D$, $a'c'=b'^2-D$, $a''b''=b''^2-D$, ... gesetzt wird, so wird die Form (A, B, C) aus den Formen (a, b, c), (a', b', c'), (a'', b'', c''), ... zusammengesetzt oder in diese Formen zerlegbar sein. Man beweist ohne Schwierigkeit, dass derselbe Satz auch noch gilt, wenn die Form (A, B, C) eine uneigentlich primitive oder eine abgeleitete Form ist. Auf diese Weise kann daher jede beliebige Form in andere mit derselben Determinante zerlegt werden, deren Anfangsglieder sämtlich entweder Primzahlen oder Potenzen von Primzahlen sind. Eine derartige Zerlegung lässt sich häufig mit Vorteil anwenden, wenn aus mehreren gegebenen Formen eine einzige zu componieren ist. So zerlege man z. B., wenn die aus den Formen (3, 1, 134), (10, 3, 41), (15, 2, 27) zusammengesetzte Form gesucht wird, die zweite in die folgenden: (2, 1, 201), (5, —2, 81), die dritte in (3, —1, 134), (5, 2, 81), dann wird offenbar die aus den fünf Formen (3, 1, 134), (2, 1, 201), (5, —2, 81), (3, —1, 134), (5, 2, 81) zusammengesetzte Form, in welcher Reihenfolge auch diese Formen genommen worden sein mögen, auch aus den drei gegebenen Formen zusammengesetzt sein. Aus der Composition der ersten und vierten aber entsteht die Hauptform (1, 0, 401); dieselbe entsteht aus der Composition der dritten und fünften; mithin ergiebt sich aus der Composition aller die Form (2, 1, 201).

5. Wegen des grossen Nutzens dieses Gegenstandes verlohnt es sich, dieses Verfahren noch etwas weiter zu entwickeln. Aus der vorigen Bemerkung geht hervor, dass das Problem, beliebig viele gegebene eigentlich primitive Formen mit derselben Determinante zusammenzusetzen, zurückgeführt werden kann auf die Composition von Formen, deren Anfangsglieder Potenzen von Primzahlen sind (denn eine Primzahl allein kann als erste Potenz von sich selbst betrachtet werden). Daher wollen wir den Fall insbesondere betrachten, wo zwei eigentlich primitive Formen (a, b, c), (a', b', c') zu componieren sind, in denen a und a' Potenzen derselben Primzahl sind. Ist also $a = h^\varkappa$, $a' = h^\lambda$, wo h eine Primzahl bezeichnet, und nehmen wir an (was erlaubt ist), dass $\varkappa$ nicht kleiner als λ sei, so wird h^λ der grösste gemeinschaftliche Teiler der Zahlen a, a', und wenn dieser überdies in $b + b'$ aufgeht, so hat man den im Anfang dieses Artikels betrachteten Fall und es wird (A, B, C) aus den gegebenen Formen zusammengesetzt sein, wenn man $A = h^{\varkappa-\lambda}$, $B \equiv b$ (mod. $h^{\varkappa-\lambda}$) und $\equiv b'$ (mod. 1), welche letztere Bedingung offenbar weggelassen werden kann, und $C = \frac{B^2 - D}{A}$ setzt. Wenn aber h^λ in $b + b'$ nicht aufgeht, so wird notwendig der grösste gemeinschaftliche Teiler dieser Zahlen auch selbst eine Potenz von h sein; ist derselbe gleich h^ν, so ist $\nu < \lambda$ (man muss $\nu = 0$ setzen, wenn zufällig h^λ und $b + b'$ prim zu einander sind). Wenn man also $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ derartig bestimmt, dass

$$\mathfrak{P}'h^\varkappa + \mathfrak{P}''h^\lambda + \mathfrak{P}'''(b + b') = h^\nu$$

wird, $\mathfrak{P}$ aber nach Belieben annimmt, so wird die Form (A, B, C) aus den gegebenen zusammengesetzt sein, wenn man setzt:

$$A = h^{\varkappa+\lambda-2\nu},\ B = b + h^{\varkappa-\nu}[\mathfrak{P}h^\lambda - \mathfrak{P}'(b' - b) - \mathfrak{P}'''c],\ C = \frac{B^2 - D}{A}.$$

Man erkennt aber leicht, dass in diesem Falle auch $\mathfrak{P}'$ willkürlich angenommen werden kann, so dass man, wenn man $\mathfrak{P} = \mathfrak{P}' = 0$ setzt, erhält:

$$B = b - \mathfrak{P}'''ch^{\varkappa-\nu},$$

oder allgemein:

$$B = kA + b - \mathfrak{P}'''ch^{\varkappa-\nu},$$

wo k eine beliebige Zahl bezeichnet (voriger Artikel). In diese sehr einfache Formel geht nur $\mathfrak{P}'''$ ein, welches der Wert des Ausdrucks $\frac{h^\nu}{b + b'}$ (mod. h^λ) ist.*) Sucht man z. B. die aus den Formen (16, 3, 19) und

*) Oder des Ausdrucks $\frac{1}{\frac{b + b'}{h^\nu}}$ (mod. $h^{\lambda-\nu}$), woraus folgt: $B \equiv b - \frac{ch^{\varkappa-\nu}}{\frac{b + b'}{h^\nu}}$ $\equiv \frac{(D + bb') : h^\nu}{(b + b') : h^\nu}$ (mod. A).

(8, 1, 37) zusammengesetzte Form, so ist $h = 2$, $\varkappa = 4$, $\gamma = 3$, $\nu = 2$. Daher $A = 8$, $\mathfrak{P}'''$ ein Wert des Ausdrucks $\frac{4}{4}$ (mod. 8); ein solcher ist 1, daher $B = 8k - 73$ und somit, wenn man $k = 9$ setzt, $B = -1$ und $C = 37$. Es ist daher (8, $-$1, 37) die gesuchte Form.

Sind also beliebig viele Formen, deren Anfangsglieder sämtlich Potenzen von Primzahlen sind, gegeben, so muss man nachsehen, ob die Anfangsglieder einiger von ihnen Potenzen derselben Primzahl sind, und diese nach der eben angebenen Regel unter sich zusammensetzen. Auf diese Weise erhält man Formen, deren erste Glieder auch noch Potenzen von Primzahlen, aber von gänzlich verschiedenen Primzahlen sind; die aus diesen zusammengesetzte Form wird daher nach der dritten Bemerkung bestimmt werden können. Sind z. B. die Formen (3, 1, 17), (4, 0, 35), (5, 0, 28), (16, 2, 9), (9, 7, 21), (16, 6, 11) gegeben, so entsteht aus der ersten und fünften die Form (27, 7, 7), aus der zweiten und vierten die Form (16, $-$6, 11), aus dieser und der sechsten die Form (1, 0, 140), welche weggelassen werden kann. Es bleiben daher übrig die Formen (5, 0, 28) und (27, 7, 7), aus denen sich die Form (135, $-$20, 4) ergiebt, an deren Stelle auch die eigentlich äquivalente Form (4, 0, 35) genommen werden kann. Dies ist also die aus der Composition der sechs gegebenen resultierende Form.

Übrigens können aus dieser Quelle noch viele andere bei der Anwendung nützliche Kunstgriffe geschöpft werden; um aber nicht allzu weitläufig zu werden, unterdrücken wir eine eingehendere Behandlung dieses Gegenstandes und wenden uns zu anderen schwierigeren Sachen.

244.

Wenn die Zahl a durch irgend eine Form f, die Zahl a' durch die Form f' dargestellt werden kann, und die Form F in ff' transformierbar ist, so ist ohne Schwierigkeit ersichtlich, dass das Product aa' durch die Form F darstellbar ist. Hieraus folgt sogleich, dass, wenn die Determinanten dieser Formen negativ sind, die Form F positiv ist, wenn entweder beide Formen f, f' positiv oder beide negativ sind, dass dagegen die Form F negativ ist, wenn die eine der Formen f, f' positiv, die andere negativ ist. Wir wollen besonders bei dem Falle verweilen, den wir im vorigen Artikel betrachtet haben, wo F aus f, f' zusammengesetzt ist und f, f', F dieselbe Determinante D haben. Nehmen wir überdies an, dass die Darstellungen der Zahlen a, a' durch die Formen f, f' vermittelst unter einander primer Werte der Unbestimmten bewirkt werden, und dass die erstere zu dem Werte b des Ausdrucks $\sqrt{D}$ (mod. a), die letztere zu dem Werte b' des Ausdrucks $\sqrt{D}$ (mod. a') gehört, und setzt man $b^2 - D = ac$, $b'^2 - D = a'c'$, so werden nach Artikel 168 die Formen (a, b, c), (a', b', c') eigentlich äquivalent sein den Formen f, f', weshalb F auch aus jenen beiden Formen zusammengesetzt sein wird. Aus denselben Formen ist aber die Form (A, B, C) zu-

sammengesetzt, wenn man, nachdem der grösste gemeinschaftliche Teiler der Zahlen a, a', $b+b'$ mit μ bezeichnet ist, $A=\frac{aa'}{\mu^2}$, $B\equiv b$ und $\equiv b'$ nach den Moduln $\frac{a}{\mu}$, $\frac{a'}{\mu}$ respective und $AC=B^2-D$ setzt. Daher wird diese Form der Form F eigentlich äquivalent sein. Nun wird die Zahl aa' durch die Form $Ax^2+2Bxy+Cy^2$ dargestellt, wenn man $x=\mu$, $y=0$ setzt, welche Werte den gemeinschaftlichen Teiler μ haben; daher lässt sich auch aa' durch die Form F derart darstellen, dass die Werte der Unbestimmten den grössten gemeinschaftlichen Teiler μ haben (Artikel 166). So oft daher $\mu=1$ ist, wird die Zahl aa' durch die Form F dargestellt werden können, indem man den Unbestimmten zu einander prime Werte beilegt, und diese Darstellung wird zu dem Werte B des Ausdrucks $\sqrt{D}$ (mod. aa') gehören, der den Zahlen b, b' respective nach den Moduln a, a' congruent ist. Die Bedingung $\mu=1$ findet immer statt, wenn a, a' prim zu einander sind; allgemein aber immer, wenn der grösste gemeinschaftliche Teiler von a, a' prim zu $b+b'$ ist.

Composition der Ordnungen.

245.

Satz. Wenn die Form f zu derselben Ordnung gehört wie g und ebenso f' aus derselben Ordnung ist wie g', so wird die aus f, f' zusammengesetzte Form F dieselbe Determinante haben und aus derselben Ordnung sein, wie die aus g, g' zusammengesetzte Form G.

Beweis. Es seien die Formen f, f', F respective gleich (a, b, c), (a', b', c'), (A, B, C) und ihre Determinanten bezüglich gleich d, d', D. Ferner sei der grösste gemeinschaftliche Teiler der Zahlen a, $2b$, c gleich m, der grösste gemeinschaftliche Teiler der Zahlen a, b, c aber gleich $\mathfrak{m}$, und analoge Bedeutungen mögen m', $\mathfrak{m}'$ in Bezug auf die Form f' und M, $\mathfrak{M}$ in Bezug auf die Form F haben. Dann wird die Ordnung der Form f durch die Zahlen d, m, $\mathfrak{m}$ bestimmt, weshalb dieselben Zahlen auch für die Form g gelten werden; aus demselben Grunde werden die Zahlen d', m', $\mathfrak{m}'$ für die Form g' dieselben sein, wie für die Form f' Nun sind aber dem Artikel 235 zufolge die Zahlen D, M, $\mathfrak{M}$ durch die Zahlen d, d', m, $\mathfrak{m}'$, $\mathfrak{m}$, $\mathfrak{m}'$ bestimmt; es ist nämlich D der grösste gemeinschaftliche Teiler von dm'^2, $d'm^2$, ferner $M=mm'$ und $\mathfrak{M}=\mathfrak{m}\mathfrak{m}'$ (wenn gleichzeitig $m=\mathfrak{m}$ und $m'=\mathfrak{m}'$ ist) oder $=2\mathfrak{m}\mathfrak{m}'$ (wenn $m=2\mathfrak{m}$ oder $m'=2\mathfrak{m}'$ ist). Da diese Eigenschaften der Zahlen D, M, $\mathfrak{M}$ daraus sich ergeben, dass F aus f, f' zusammengesetzt ist, so ist leicht ersichtlich, dass D, M, $\mathfrak{M}$ auch für die Form G gelten und daher G aus derselben Ordnung ist wie F. W. z. B. w.

Aus diesem Grunde werden wir die Ordnung, in welcher F enthalten ist, aus den Ordnungen, in denen f, f' enthalten sind,

zusammengesetzt nennen. So ist z. B. aus zwei eigentlich primitiven Ordnungen immer eine Ordnung gleicher Art, aus einer eigentlich primitiven und einer uneigentlich primitiven eine uneigentlich primitive Ordnung zusammengesetzt. — In analoger Weise hat man es zu verstehen, wenn eine Ordnung aus mehreren anderen Ordnungen zusammengesetzt genannt wird.

Composition der Geschlechter.

246.

Aufgabe. Wenn zwei beliebige primitive Formen f, f', aus deren Composition die Form F entsteht, gegeben sind, so soll man aus den Geschlechtern, zu welchen f, f' gehören, das Geschlecht bestimmen, zu welchem F zu rechnen ist.

Auflösung. I. Wir betrachten zunächst den Fall, wo wenigstens eine der Formen f, f', z. B. die erstere, eigentlich primitiv ist, und bezeichnen die Determinanten der Formen f, f', F bezüglich mit d, d', D. Dann ist D der grösste gemeinschaftliche Teiler der Zahlen dm'^2, d', wo m' entweder gleich 1 oder gleich 2 ist, je nachdem die Form f' eigentlich oder uneigentlich primitiv ist. Im ersten Falle wird F zu einer eigentlich primitiven Ordnung, im zweiten zu einer uneigentlich primitiven Ordnung gehören. Nun wird das Geschlecht der Form F bestimmt durch ihre Specialcharactere sowohl in Bezug auf die einzelnen ungeraden Primteiler von D als auch für gewisse Fälle in Bezug auf die Zahlen 4 und 8. Diese müssen wir daher einzeln bestimmen.

1. Ist p irgend ein ungerader Primteiler von D, so geht derselbe notwendig auch in d, d' auf und daher werden auch unter den Characteren der Formen f, f' die Beziehungen dieser zu p vorkommen. Wenn nun durch f eine Zahl a, durch f' eine Zahl a' dargestellt werden kann, so wird das Product aa' durch F darstellbar sein. Wenn daher sowohl durch f als auch durch f' quadratische (durch p nicht teilbare) Reste von p dargestellt werden können, so können auch durch F quadratische Reste von p dargestellt werden, d. h. wenn jede der beiden Formen f, f' den Character Rp hat, so wird auch die Form F denselben Character haben. Aus demselben Grunde wird F den Character Rp haben, wenn jede der beiden Formen f, f' den Character Np hat; dagegen hat F den Character Np, wenn eine der beiden Formen f, f' den Character Rp, die andere den Character Np hat.

2. Wenn in den Totalcharacter der Form F die Beziehung zur Zahl 4 eingeht, so muss eine solche Beziehung auch in die Charactere der Formen f, f' eintreten. Denn jenes findet nur dann statt, wenn $D \equiv 0$ oder $\equiv 3 \pmod{4}$ ist. Ist D durch 4 teilbar, so sind auch dm'^2 und d' durch 4 teilbar, woraus sogleich hervorgeht, dass f' nicht uneigentlich primitiv sein kann und somit $m' = 1$ ist. Daher ist sowohl d als d' durch 4 teilbar,

und in den Character beider Formen tritt die Beziehung zu 4 ein. Ist $D \equiv 3$ (mod. 4), so geht D in d, d' auf; die Quotienten sind Quadrate und daher auch d, d' notwendig entweder $\equiv 0$ oder $\equiv 3$ (mod. 4), und unter den Characteren von f, f' findet sich ihre Beziehung zu 4. Hieraus folgt in derselben Weise wie in (1), dass der Character der Form f 1, 4 ist, wenn entweder beide Formen f, f' den Character 1, 4 oder den Character 3, 4 haben, dass dagegen der Character der Form F 3, 4 ist, wenn die eine der Formen f, f' den Character 1, 4, die andere den Character 3, 4 hat.

3. Ist D durch 8 teilbar, so ist es auch d'; demnach ist f' sicher eigentlich primitiv, $m' = 1$ und auch d durch 8 teilbar. Daher kann unter den Characteren der Form F irgend einer der Charactere 1, 8; 3, 8; 5, 8; 7, 8 nur dann sich vorfinden, wenn auch in dem Character der Form f sowohl als in dem Character der Form f' eine solche Beziehung zu 8 vorkommt. Man bestätigt aber leicht in derselben Weise wie vorher, dass der Character der Form F 1, 8 ist, wenn f und f' in Bezug auf 8 denselben Character haben; dass der Character der Form F 3, 8 ist, wenn die eine der Formen f, f' den Character 1, 8, die andere den Character 3, 8, oder die eine den Character 5, 8, die andere den Character 7, 8 hat; dass die Form F den Character 5, 8 besitzt, wenn die Formen f, f' die Charactere 1, 8 und 5, 8 oder die Charactere 3, 8 und 7, 8 haben; dass endlich F den Character 7, 8 hat, wenn f, f' die Charactere 1, 8 und 7, 8 oder 3, 8 und 5, 8 haben.

4. Ist $D \equiv 2$ (mod. 8), so ist d' entweder $\equiv 0$ oder $\equiv 2$ (mod. 8); demnach ist $m' = 1$ und daher auch d entweder $\equiv 0$ oder $\equiv 2$ (mod. 8). Indessen können nicht beide Zahlen d, d' durch 8 teilbar sein, da D der grösste gemeinschaftliche Teiler derselben ist. Daher wird nur in dem Falle der eine oder der andere der beiden Charactere 1 u. 7, 8; 3 u. 5, 8 der Form F zuerteilt werden dürfen, wenn entweder beide Formen f, f' irgend einen von jenen Characteren besitzen, oder die eine einen von jenen, die andere einen der folgenden Charactere 1, 8; 3, 8; 5, 8; 7, 8 hat. Hieraus ergiebt sich leicht, dass der Character der Form F durch die folgende Tafel bestimmt werden kann, wenn sich der am Rande befindliche Character auf die eine der beiden Formen f, f', der am Kopfe befindliche aber auf die andere bezieht:

	1 u. 7, 8 oder 1, 8 oder 7, 8	3 u. 5, 8 oder 3, 8 oder 5, 8
1 u. 7, 8	1 u. 7, 8	3 u. 5, 8
3 u. 5, 8	3 u. 5, 8	1 u. 7, 8

5. Auf dieselbe Art beweist man, dass der Form F der eine oder der andere der beiden Charactere 1 u. 3, 8; 5 u. 7, 8 nicht beigelegt werden

kann, wenn nicht irgend einer von ihnen wenigstens einer der Formen *f*, *f'* und der andern entweder einer von denselben Characteren oder einer von den folgenden: 1, 8; 3, 8; 5, 8; 7, 8 zukommt, und zwar bestimmt sich der Character der Form F durch folgende Tafel, bei welcher sich die Charactere der Formen *f*, *f'* am Rande und am Kopfe befinden:

	1 u. 3, 8 oder 1, 8 oder 3, 8	5 u. 7, 8 oder 5, 8 oder 7, 8
1 u. 3, 8	1 u. 3, 8	5 u. 7, 8
5 u. 7, 8	5 u. 7, 8	1 u. 3, 8

II. Wenn beide Formen *f*, *f'* uneigentlich primitiv sind, so ist D der grösste gemeinschaftliche Teiler der Zahlen $4d$, $4d'$ oder $\frac{1}{4}D$ der grösste gemeinschaftliche Teiler der Zahlen d, d'. Hieraus folgt leicht, dass sowohl d als auch d' als auch $\frac{1}{4}D \equiv 1$ (mod. 4) sind. Setzt man aber $F = (A, B, C)$, so ist der grösste gemeinschaftliche Teiler der Zahlen A, B, C gleich 2 und der grösste gemeinschaftliche Teiler der Zahlen A, $2B$, C gleich 4. Daher ist F eine aus der uneigentlich primitiven Form $(\frac{1}{2}A, \frac{1}{2}B, \frac{1}{2}C)$ abgeleitete Form; die Determinante der letzteren ist $\frac{1}{4}D$ und ihr Geschlecht wird das Geschlecht der Form F bestimmen. Der Character jener Form aber wird, da sie eine uneigentlich primitive ist, die Beziehungen zu 4 oder 8 nicht enthalten, sondern nur die Beziehungen zu den einzelnen ungeraden Primteilern von $\frac{1}{4}D$. Da nun offenbar alle diese Teiler in d, d' aufgehen und die Hälfte eines jeden Productes zweier Factoren, von denen der eine durch *f*, der andere durch *f'* darstellbar ist, durch die Form $(\frac{1}{2}A, \frac{1}{2}B, \frac{1}{2}C)$ dargestellt werden kann, so sieht man leicht, dass der Character dieser Form in Bezug auf jede in $\frac{1}{4}D$ aufgehende ungerade Primzahl p Rp ist, sowohl wenn $2Rp$ ist und die Formen *f*, *f'* in Bezug auf p ein und denselben Character haben, als auch wenn $2Np$ ist und die Charactere der Formen *f*, *f'* in Bezug auf p entgegengesetzt sind, dass dagegen der Character jener Form Np ist, sowohl wenn *f*, *f'* gleiche Charactere haben in Bezug auf p und $2Np$ ist, als auch wenn *f*, *f'* entgegengesetzte Charactere haben und $2Rp$ ist.

247.

Aus der Auflösung des vorstehenden Problems geht hervor, dass, wenn g eine primitive Form aus derselben Ordnung und demselben Geschlechte wie *f* und ebenso g' eine primitive Form aus derselben Ordnung und demselben Geschlechte wie *f'* ist, die aus g und g' zusammengesetzte Form zu demselben Geschlechte gehört wie die aus *f* und *f'* zusammengesetzte Form. Hieraus ergiebt sich unmittelbar die Bedeutung eines aus zwei (oder auch aus mehreren) andern Geschlechtern **zusammengesetzten Geschlechts.**

Ferner geht ebendaraus hervor, dass, wenn f, f' dieselbe Determinante haben und f eine Form aus einem Hauptgeschlechte, sowie F aus f und f' zusammengesetzt ist, F aus demselben Geschlechte ist wie f'; demnach kann ein Hauptgeschlecht bei der Composition mit andern Geschlechtern derselben Determinante stets weggelassen werden. Wenn dagegen, während die übrigen Annahmen bleiben, f nicht aus einem Hauptgeschlecht, f' aber eine primitive Form ist, so wird F sicher aus einem andern Geschlechte sein als f'. Wenn endlich f, f' eigentlich primitive Formen desselben Geschlechts sind, so wird F aus einem Hauptgeschlechte sein; wenn dagegen f, f' beide eigentlich primitive Formen mit derselben Determinante, aber aus verschiedenen Geschlechtern sind, so kann F nicht zu einem Hauptgeschlechte gehören. Wird daher irgend eine eigentlich primitive Form mit sich selbst componiert, so wird die dadurch entstehende Form, welche ebenfalls eigentlich primitiv ist und dieselbe Determinante hat, notwendig zu einem Hauptgeschlechte gehören.

248.

Aufgabe. Wenn zwei beliebige Formen f, f', aus denen die Form F zusammengesetzt ist, gegeben sind, so soll man aus den Geschlechtern der Formen f, f' bestimmen, zu welchem Geschlechte die Form F gehört.

Auflösung. Es sei $f=(a, b, c)$, $f'=(a', b', c')$, $F=(A, B, C)$, ferner $\mathfrak{m}$ der grösste gemeinschaftliche Teiler der Zahlen a, b, c und $\mathfrak{m}'$ der grösste gemeinschaftliche Teiler der Zahlen a', b', c', so dass f, f' aus den primitiven Formen $\left(\frac{a}{\mathfrak{m}}, \frac{b}{\mathfrak{m}}, \frac{c}{\mathfrak{m}}\right)$, $\left(\frac{a'}{\mathfrak{m}'}, \frac{b'}{\mathfrak{m}'}, \frac{c'}{\mathfrak{m}'}\right)$, die wir bezüglich mit $\mathfrak{f}, \mathfrak{f}'$ bezeichnen, abgeleitet sind. Wenn nun wenigstens eine der Formen $\mathfrak{f}, \mathfrak{f}'$ eigentlich primitiv ist, so wird der grösste gemeinschaftliche Teiler der Zahlen A, B, C gleich $\mathfrak{m}\mathfrak{m}'$ und daher F aus der primitiven Form $\left(\frac{A}{\mathfrak{m}\mathfrak{m}'}, \frac{B}{\mathfrak{m}\mathfrak{m}'}, \frac{C}{\mathfrak{m}\mathfrak{m}'}\right)=\mathfrak{F}$ abgeleitet sein, woraus hervorgeht, dass das Geschlecht der Form F abhängig ist vom Geschlecht der Form $\mathfrak{F}$. Man erkennt aber leicht, dass $\mathfrak{F}$ durch dieselbe Substitution in $\mathfrak{f}\mathfrak{f}'$ übergeht, durch welche F in ff' übergeht und dass somit $\mathfrak{F}$ aus $\mathfrak{f}\mathfrak{f}'$ zusammengesetzt ist und ihr Geschlecht nach der Aufgabe im Artikel 246 bestimmt werden kann. — Sind aber beide Eormen $\mathfrak{f}, \mathfrak{f}'$ uneigentlich primitiv, so ist der grösste gemeinschaftliche Teiler der Zahlen A, B, C gleich $2\mathfrak{m}\mathfrak{m}'$ und die Form $\mathfrak{F}$ ist auch jetzt noch aus den Formen $\mathfrak{f}, \mathfrak{f}'$ zusammengesetzt und offenbar aus der eigentlich primitiven Form $\left(\frac{A}{2\mathfrak{m}\mathfrak{m}'}, \frac{B}{2\mathfrak{m}\mathfrak{m}'}, \frac{C}{2\mathfrak{m}\mathfrak{m}'}\right)$ abgeleitet. Das Geschlecht dieser Form kann daher nach Artikel 246 bestimmt werden, und da F aus eben dieser Form abgeleitet ist, so wird dadurch auch unmittelbar das Geschlecht von F bekannt sein.

Aus dieser Auflösung geht hervor, dass der im vorigen Artikel für primitive Formen entwickelte Satz, nämlich dass, wenn f', g' aus den-

selben Geschlechtern sind, wie f, g, die aus den Formen f', g' zusammengesetzte Form aus demselben Geschlechte ist, wie die aus f, g zusammengesetzte Form, allgemein für beliebige Formen gilt.

Composition der Klassen.

249.

Satz. Wenn die Formen f, f' aus denselben Ordnungen, Geschlechtern und Klassen sind, wie die Formen g, g' respective, so ist die aus den Formen f, f' zusammengesetzte Form aus derselben Klasse, wie die aus g und g' zusammengesetzte.

Aus diesem Satze, dessen Richtigkeit aus Artikel 239 ohne Weiteres folgt, ist die Bedeutung einer aus zwei oder auch aus mehreren gegebenen Klassen **zusammengesetzten Klasse** unmittelbar ersichtlich.

Wird irgend eine Klasse K mit der Hauptklasse zusammengesetzt, so entsteht wiederum die Klasse K, d. h. die Hauptklasse kann bei der Composition mit andern Klassen derselben Determinante weggelassen werden. Aus der Composition zweier entgegengesetzten eigentlich primitiven Klassen entsteht stets die Hauptklasse derselben Determinante (vgl. Artikel 243). Da nun jede ambige Klasse sich selbst entgegengesetzt ist, so geht durch Composition jeder eigentlich primitiven ambigen Klasse mit sich selbst die Hauptklasse derselben Determinante hervor.

Der letzte Satz gilt auch umgekehrt, nämlich: Wenn durch Composition einer eigentlich primitiven Klasse K mit sich selbst die Hauptklasse H derselben Determinante hervorgeht, so ist K notwendig eine ambige Klasse. Denn wenn K' die zu K entgegengesetzte Klasse ist, so wird aus den drei Klassen K, K, K' durch Composition dieselbe Klasse entstehen wie aus H und K'; aus jenen ergiebt sich aber K (da K und K' die Hauptklasse H, diese aber und K wiederum K hervorbringen), aus diesen K'. Mithin fällt K mit K' zusammen und ist daher eine ambige Klasse.

Ferner mag folgender Satz angeführt werden: Wenn die Klassen K, L bezüglich den Klassen K', L' entgegengesetzt sind, so wird auch die aus K und L zusammengesetzte Klasse der aus K' und L' zusammengesetzten entgegengesetzt sein. Es seien die Formen f, g, f', g' bezüglich aus den Klassen K, L, K', L'; die Form F sei aus f und g, die Form F' aus den Formen f' und g' zusammengesetzt. Da f' und f sowie g' und g uneigentlich äquivalent sind, F aber aus jeder der beiden Formen f, g direct zusammengesetzt ist, so wird F auch aus f', g' zusammengesetzt sein, aber aus jeder der beiden invers. Daher ist jede Form, welche F uneigentlich äquivalent ist, aus f' und g' direct zusammengesetzt und daher der Form F' eigentlich äquivalent (Artikel 238, 239),

weshalb F, F' uneigentlich äquivalent und die Klassen, zu denen sie gehören, entgegengesetzt sind.

Hieraus folgt, dass, wenn eine ambige Klasse K mit einer ambigen Klasse L zusammengesetzt wird, immer eine ambige Klasse entsteht. Denn dieselbe ist der Klasse, welche aus den den Klassen K, L entgegengesetzten Klassen zusammengesetzt ist, und daher sich selbst entgegengesetzt, da diese Klassen sich selbst entgegengesetzt sind.

Endlich bemerken wir, dass, wenn zwei beliebige Klassen K, L mit derselben Determinante gegeben sind, von denen die erste eigentlich primitiv ist, man immer eine Klasse M mit derselben Determinante finden kann, welche mit K componiert L ergiebt. Offenbar erreicht man dies, indem man für M die Klasse nimmt, welche aus L und der zu K entgegengesetzten Klasse zusammengesetzt ist; zugleich ist sehr leicht ersichtlich, dass diese Klasse die einzige ist, welche diese Eigenschaft besitzt, oder dass verschiedene Klassen derselben Determinante mit einer und derselben eigentlich primitiven Klasse zusammengesetzt verschiedene Klassen liefern.

Die Composition der Klassen kann passend durch das Additionszeichen $+$, ebenso wie die Identität der Klassen durch das Gleichheitszeichen, bezeichnet werden. In diesen Zeichen lässt sich der eben angegebene Satz folgendermassen ausdrücken: Wenn K' die zu K entgegengesetzte Klasse ist, so ist $K+K'$ die Hauptklasse derselben Determinante, und somit $K+K'+L=L$; setzt man also $K'+L=M$, so ist $K+M=L$, wie verlangt wurde. Wenn es aber ausser M noch eine andere M' gäbe, welche dieselbe Eigenschaft besässe, oder wenn $K+M'=L$ wäre, so würde $K+K'+M'=L+K'=M$ sein, woraus $M'=M$ folgt. — Wenn mehrere identische Klassen zusammengesetzt werden, so kann dies (nach Art der Multiplikation) durch Vorsetzen ihrer Anzahl bezeichnet werden, so dass z. B. $2K$ dasselbe bezeichnet wie $K+K$, $3K$ dasselbe wie $K+K+K$, u. s. w. Dieselben Bezeichnungen können auch auf die Formen übertragen werden, so dass $(a, b, c)+(a', b', c')$ die aus (a, b, c), (a', b', c') zusammengesetzte Form bezeichnen würde; um aber keine Zweideutigkeit aufkommen zu lassen, wollen wir uns dieser Abkürzung lieber enthalten, zumal wir einem Zeichen wie $\sqrt{M(a, b, c)}$ schon eine besondere Bedeutung beigelegt haben. — Wir werden sagen, dass die Klasse $2K$ durch **Duplikation** der Klasse K, die Klasse $3K$ durch **Triplikation** von K u. s. w. entstehe.

250.

Wenn D eine durch m^2 teilbare Zahl ist (wo wir m als positiv voraussetzen), so giebt es eine aus einer eigentlich primitiven Ordnung mit der Determinante $\frac{D}{m^2}$ abgeleitete Ordnung der Formen mit der Determinante D (oder zwei, falls D negativ ist, nämlich eine positive und eine negative). Offenbar wird die Form $\left(m, 0, -\frac{D}{m}\right)$ zu jener Ordnung (nämlich der posi-

tiven) gehören und kann mit Recht als die einfachste Form in derselben betrachtet werden (ebenso wie $\left(-m, 0, \frac{D}{m}\right)$ im Falle eines negativen D die einfachste Form in der negativen Ordnung sein wird). Wenn überdies $\frac{D}{m^2} \equiv 1 \pmod{4}$ ist, so giebt es auch eine Ordnung von Formen mit der Determinante D, welche aus der uneigentlich primitiven Ordnung mit der Determinante $\frac{D}{m^2}$ abgeleitet ist und zu der offenbar die Form $\left(2m, m, \frac{m^2-D}{2m}\right)$ gehören und in ihr für die einfachste gehalten werden wird. (Ist D negativ, so giebt es wiederum zwei Ordnungen und in der negativen soll die Form $\left(-2m, -m, \frac{D-m^2}{2m}\right)$ als die einfachste betrachtet werden). So werden z. B., wenn wir auch den Fall, wo $m = 1$ ist, hierher rechnen wollen, in den vier Ordnungen von Formen mit der Determinante 45 die folgenden Formen die einfachsten sein: $(1, 0, -45)$, $(2, 1, -22)$, $(3, 0, -15)$, $(6, 3, -6)$. In diesem Sinn ist der folgende Satz zu verstehen:

Satz. Wenn irgend eine Form F aus der Ordnung O gegeben ist, so soll man eine eigentlich primitive (positive) Form finden, durch deren Composition mit der einfachsten Form in O die Form F entsteht.

Auflösung. Es sei die Form $F = (ma, mb, mc)$ aus der primitiven Form $f = (a, b, c)$, deren Determinante gleich d ist, abgeleitet und es werde zunächst angenommen, dass f eigentlich primitiv sei. Wir bemerken zunächst, dass, wenn etwa a nicht prim zu $2dm$ ist, es sicher andere zu (a, b, c) eigentlich äquivalente Formen giebt, welche diese Eigenschaft besitzen. Denn nach Artikel 228 giebt es zu $2dm$ prime und durch jene Form darstellbare Zahlen; es sei eine solche Zahl $a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2$, und es werde (was erlaubt ist) angenommen, dass α, γ prim zu einander sind. Werden dann β, δ derart angenommen, dass $\alpha\delta - \beta\gamma = 1$ ist, so möge f durch die Substitution $\alpha, \beta, \gamma, \delta$ in die Form (a', b', c') übergehen, welche jener eigentlich äquivalent sein und die vorgeschriebene Eigenschaft haben wird. Da nun auch F und $(a'm, b'm, c'm)$ eigentlich äquivalent sind, so sieht man leicht, dass es genügt denjenigen Fall zu betrachten, in welchem a zu $2dm$ prim ist. Dann wird (a, bm, cm^2) eine eigentlich primitive Form (denn wenn a, $2bm$, cm^2 einen gemeinschaftlichen Teiler hätten, so würde derselbe auch in $2dm = 2b^2m - 2acm$ enthalten sein) mit derselben Determinante wie F sein, und man bestätigt leicht, dass die Form F durch die Substitution $1, 0, -b, -cm; 0, m, a, bm$ in das Product aus der Form $(m, 0, -dm)$, welche, wenn F nicht eine negative Form ist, die einfachste der Ordnung O ist, und der Form (a, bm, cm^2) übergeht, woraus man aus dem Kriterium in der vierten Bemerkung des Artikels 235 schliesst, dass F aus $(m, 0, -dm)$ und (a, bm, cm^2) zusammengesetzt ist. Ist aber F eine negative Form, so geht sie in das Product aus der einfachsten Form der-

selben Ordnung $(-m, 0, dm)$ und der positiven Form $(-a, bm, -cm^2)$ über durch die Substitution $1, 0, b, -cm; 0, -m, -a, bm$ und ist daher aus ihnen zusammengesetzt.

Ist zweitens f eine uneigentlich primitive Form, so kann man annehmen, dass $\frac{1}{2}a$ und $2dm$ prim zu einander sind; denn wenn diese Eigenschaft bei der Form f nicht stattfindet, so kann man eine f eigentlich äquivalente Form finden, welche diese Eigenschaft besitzt. Hieraus aber folgt leicht, dass $(\frac{1}{2}a, bm, 2cm^2)$ eine eigentlich primitive Form mit derselben Determinante wie F ist, und ebenso leicht bestätigt man, dass F in das Product der beiden Formen

$$\left(\pm 2m, \pm m, \pm \tfrac{1}{2}(m - dm)\right), \quad \left(\pm \tfrac{1}{2}a, bm, \pm 2cm^2\right)$$

übergeht durch die Substitution:

$$1, 0, \tfrac{1}{2}(1 \mp b), -cm; \quad 0, \pm 2m, \pm \tfrac{1}{2}a, (b \pm 1)m,$$

wobei die unteren Zeichen zu nehmen sind, wenn F eine negative Form ist, die oberen aber in den übrigen Fällen, und dass somit F aus diesen beiden Formen, von denen die erste die einfachste der Ordnung O, die letzte eine eigentlich primitive (positive) Form ist, zusammengesetzt ist.

251.

Aufgabe. Wenn zwei Formen F, f mit derselben Determinante D, welche zu derselben Ordnung O gehören, gegeben sind, so soll man eine eigentlich primitive Form mit der Determinante D finden, welche mit f componiert die Form F erzeugt.

Auflösung. Es sei φ die einfachste Form der Ordnung O; ferner seien $\mathfrak{F}, \mathfrak{f}$ eigentlich primitive Formen mit der Determinante D, welche mit φ componiert bezüglich F, f hervorbringen; endlich sei f' eine eigentlich primitive Form, welche mit $\mathfrak{f}$ componiert die Form $\mathfrak{F}$ erzeugt. Dann wird die Form F aus den drei Functionen $\varphi, \mathfrak{f}, f'$ oder aus den beiden f, f' zusammengesetzt sein.

Es kann daher jede Klasse einer gegebenen Ordnung betrachtet werden als zusammengesetzt aus irgend einer gegebenen Klasse derselben Ordnung und irgend einer eigentlich primitiven Klasse mit derselben Determinante.

Für eine gegebene Determinante sind in den einzelnen Geschlechtern derselben Ordnung gleichviele Klassen enthalten.

252.

Satz. Für eine gegebene Determinante sind in den einzelnen Geschlechtern derselben Ordnung gleichviele Klassen enthalten.

Beweis. Es mögen die Geschlechter G und H zu derselben Ordnung gehören, und es möge G aus den n Klassen $K, K', K'', \ldots, K^{(n-1)}$ be-

stehen; ferner sei L irgend eine Klasse aus dem Geschlechte H. Man suche nach dem vorigen Artikel eine eigentlich primitive Klasse M mit derselben Determinante, aus deren Composition mit K die Klasse L entsteht, und bezeichne die aus der Composition der Klasse M mit den Klassen K', K'', ..., $K^{(n-1)}$ hervorgehenden Klassen respective mit L', L'', ..., $L^{(n-1)}$. Dann folgt aus der letzten Bemerkung im Artikel 249, dass alle Klassen L, L', L'', ..., $L^{(n-1)}$ verschieden sind, und nach Artikel 248 gehören sie sämtlich zu demselben Geschlechte, d. h. zum Geschlechte H. Schliesslich sieht man leicht, dass H andere Klassen als diese nicht enthalten kann, da jede Klasse des Geschlechts H als zusammmengesetzt aus M und einer andern Klasse derselben Determinante, welche notwendig immer aus dem Geschlechte G ist, betrachtet werden kann. Daher enthält H, ebenso wie G, n verschiedene Klassen.

Die Anzahlen der in den einzelnen Geschlechtern verschiedener Ordnungen enthaltenen Klassen werden verglichen.

253.

Der vorhergehende Satz setzt die Identität der Ordnung voraus und lässt sich nicht auf verschiedene Ordnungen ausdehnen. So giebt es z. B. für die Determinante -171 zwanzig positive Klassen, welche sich auf vier Ordnungen verteilen. In der eigentlich primitiven Ordnung sind zwei Geschlechter enthalten, deren jedes sechs Klassen umfasst; in der uneigentlich primitiven Ordnung besitzen die beiden Geschlechter vier Klassen, jedes einzelne deren zwei; in der aus der eigentlich primitiven Ordnung mit der Determinante -19 abgeleiteten Ordnung giebt es nur ein einziges Geschlecht, welches drei Klassen enthält; endlich hat die aus der uneigentlich primitiven Ordnung mit der Determinante -19 abgeleitete Ordnung nur ein einziges, aus einer Klasse bestehendes Geschlecht. Ebenso verhalten sich die negativen Klassen. Es verlohnt daher der Mühe, ein allgemeines Prinzip zu suchen, von welchem der Zusammenhang unter den Klassenanzahlen in den verschiedenen Ordnungen abhängt. Wir nehmen an, dass K, L zwei Klassen aus derselben (positiven) Ordnung O mit der Determinante D seien und M eine eigentlich primitive Klasse mit derselben Determinante sei, aus deren Composition mit K die Klasse L entsteht; eine solche lässt sich nach Artikel 251 stets angeben. Nun kann es in gewissen Fällen geschehen, dass M die einzige eigentlich primitive Klasse ist, welche mit K componiert L erzeugt; in andern können mehrere verschiedene eigentlich primitive Klassen existieren, welche diese Eigenschaft besitzen. Wir nehmen allgemein an, dass es r derartige eigentlich primitive Klassen M, M', M'', . . ., $M^{(r-1)}$ giebt, welche, einzeln mit K componiert, dieselbe Klasse L hervorbringen, und bezeichnen die Gesamtheit jener mit W. Ferner sei L' eine andere (von L verschiedene) Klasse der Ordnung

O und N' die eigentlich primitive Klasse mit der Determinante D, welche mit L componiert L' erzeugt, und es werde die Gesamtheit der Klassen $N' + M$, $N' + M'$, $N' + M''$, ..., $N' + M^{(r-1)}$ (welche sämtlich eigentlich primitiv und von einander verschieden sind) mit W' bezeichnet. Dann ist leicht ersichtlich, dass K mit irgend einer Klasse aus W' componiert L' hervorbringt, woraus folgt, dass W und W' keine Klasse gemeinschaftlich haben; ausserdem zeigt man ohne Mühe, dass es keine eigentlich primitive in dem Complexe W' nicht enthaltene Klasse giebt, welche mit K componiert L' hervorbrächte. Auf dieselbe Weise erhellt, dass, wenn L'' eine andere von den Klassen L, L' verschiedene Klasse der Ordnung O ist, es r eigentlich primitive sowohl unter sich als auch von den Klassen W, W' verschiedene Klassen giebt, welche einzeln mit K componiert L'' hervorbringen, und ähnlich verhält es sich mit allen übrigen Klassen der Ordnung O. Da aber jede eigentlich primitive (positive) Klasse mit der Determinante D mit K componiert eine Klasse der Ordnung O liefert, so folgt hieraus leicht, dass, wenn die Anzahl der sämtlichen Klassen der Ordnung O gleich n ist, die Anzahl sämtlicher eigentlich primitiven (positiven) Klassen mit derselben Determinante gleich rn ist. Wir erhalten daher die allgemeine **Regel**: Bezeichnen K, L irgend welche Klassen der Ordnung O und r die Anzahl der verschiedenen eigentlich primitiven Klassen mit derselben Determinante, welche einzeln mit K componiert L erzeugen, so ist die Anzahl sämtlicher Klassen in der eigentlich primitiven (positiven) Ordnung r-mal grösser als die Anzahl der Klassen der Ordnung O.

Da die Klassen K, L in der Ordnung O ganz nach Belieben angenommen werden können, so wird man auch identische Klassen nehmen dürfen, und zwar wird es zweckmässig sein, sich derjenigen Klasse zu bedienen, in welcher die einfachste Form dieser Ordnung enthalten ist. Nimmt man daher diese für K und L, so ist die Sache darauf zurückgeführt, sämtliche eigentlich primitiven Klassen anzugeben, welche mit K componiert wiederum K erzeugen. Hierzu wird der Weg gebahnt durch den Satz des folgenden Artikels.

254.

Satz. Wenn $F = (A, B, C)$ die einfachste Form der Ordnung O mit der Determinante D und $f = (a, b, c)$ eine eigentlich primitive Form mit derselben Determinante ist, so lässt sich durch diese Form f die Zahl A^2 darstellen, wenn F durch Composition der Formen f, F entsteht, und umgekehrt ist F aus sich selbst und f zusammengesetzt, wenn A^2 durch f dargestellt werden kann.

Beweis. I. Wenn F in das Product fF durch die Substitution $p, p', p'', p'''; q, q', q'', q'''$ übergeht, so hat man nach Artikel 235:

$$A(aq''^2 - 2bqq'' + cq^2) = A^3, \text{ daher: } A^2 = aq''^2 - 2bqq'' + cq^2.$$

II. Wenn vorausgesetzt wird, dass A^2 durch f dargestellt werden könne, so bezeichne man die Werte der Unbestimmten, durch welche dies bewirkt wird, mit $q'', -q$, oder es sei: $A^2 = aq''^2 - 2bqq'' + cq^2$, und es werde gesetzt:

$$q''a - q(b+B) = Ap, \quad -qC = Ap', \quad q''(b-B) - qc = Ap''$$
$$-q''C = Ap''', \quad q''a - q(b-B) = Aq', \quad q''(b+B) - qc = Aq'''.$$

Dann zeigt man leicht, dass F in das Product fF durch die Substitution p, p', p'', p'''; q, q', q'', q''' übergeht und daher aus f und F zusammengesetzt ist, wofern nur sämtliche Zahlen $p, p', \ldots$ ganz sind. Nun ist nach der Erklärung der einfachsten Form B entweder gleich 0 oder gleich $\frac{1}{2}A$, daher ist $\frac{2B}{A}$ eine ganze Zahl; ebendaraus folgt, dass auch $\frac{C}{A}$ eine ganze Zahl ist. Demnach sind $q'-p, p', q'''-p'', p'''$ ganze Zahlen, und es bleibt daher nur zu beweisen, dass p und p'' ganze Zahlen sind. Es wird aber:

$$p^2 + \frac{2pqB}{A} = a - \frac{q^2C}{A}, \quad p''^2 + \frac{2p''q''B}{A} = c - \frac{q''^2C}{A}.$$

Ist daher $B = 0$, so folgt:

$$p^2 = a - \frac{q^2C}{A}, \quad p''^2 = c - \frac{q''^2C}{A},$$

und somit sind p und p'' ganze Zahlen; ist dagegen $B = \frac{1}{2}A$, so ist:

$$p^2 + pq = a - \frac{q^2C}{A}, \quad p''^2 + p''q'' = c - \frac{q''^2C}{A},$$

woraus ebenso leicht sich ergiebt, dass auch in diesem Falle p und p'' ganze Zahlen sind. Hieraus folgt, dass F aus f und F zusammengesetzt ist.

255.

Das Problem ist demnach darauf zurückgeführt, dass man alle eigentlich primitiven Klassen mit der Determinante D bestimmen solle, durch deren Formen die Zahl A^2 sich darstellen lässt. Offenbar ist A^2 durch jede Form darstellbar, deren erstes Glied entweder A^2 oder das Quadrat eines aliquoten Teils von A ist; umgekehrt aber wird, wenn A^2 durch die Form f dargestellt werden kann, indem man den Unbestimmten die Werte αe, γe, deren grösster gemeinschaftlicher Teiler e ist, beilegt, die Form f durch die Substitution $\alpha, \beta, \gamma, \delta$ in eine Form übergehen, deren erstes Glied $\frac{A^2}{e^2}$ ist, und diese Form wird der Form f eigentlich äquivalent sein, wenn $\alpha\delta - \beta\gamma = 1$ ist. Hieraus geht hervor, dass sich in jeder Klasse, durch deren Formen A^2 dargestellt werden kann, Formen finden, deren erstes Glied entweder A^2 oder das Quadrat eines aliquoten Teils von A ist. Die Sache dreht sich also darum, alle eigentlich primitiven Klassen mit der

Determinante D zu ermitteln, in denen derartige Formen vorkommen, und dies erreicht man auf folgende Weise: Es seien a, a', a'', ... sämtliche (positiven) Teiler von A; man suche sämtliche Werte des Ausdrucks $\sqrt{D}\,(\mathrm{mod.}\, a^2)$, welche zwischen 0 und $a^2 - 1$ incl. liegen und welche b, b', b'', ... sein mögen, und setze:

$$b^2 - D = a^2c, \quad b'^2 - D = a^2c', \quad b''^2 - D = a^2c'', \ldots;$$

ferner werde die Gesamtheit der Formen (a^2, b, c), (a^2, b', c'), ... mit V bezeichnet. Dann sieht man leicht, dass in jeder Klasse mit der Determinante D, in welcher eine Form vorkommt, deren erstes Glied a^2 ist, auch irgend eine Form aus V enthalten sein muss. In analoger Weise ermittle man sämtliche Formen mit der Determinante D, deren erstes Glied a'^2 und deren mittleres Glied zwischen 0 und $a'^2 - 1$ incl. gelegen ist, und bezeichne den Complex derselben mit V'. Ebenso sei V'' der Complex analoger Formen, deren erstes Glied a''^2 ist, u. s. w. Aus den Formen V, V', V'', ... entferne man sämtliche Formen, welche nicht eigentlich primitiv sind, verteile die übrigen in Klassen und behalte, wenn zufällig mehrere zu derselben Klasse gehörende vorhanden sein sollten, in den einzelnen Klassen nur eine bei. Auf diese Weise erhält man alle gesuchten Klassen und die Anzahl derselben wird sich zur Einheit verhalten, wie die Anzahl aller eigentlich primitiven (positiven) Klassen zur Anzahl der Klassen in der Ordnung O.

Beispiel. Es sei $D = -531$ und O die positive aus der uneigentlich primitiven Ordnung mit der Determinante -59 abgeleitete Ordnung, in welcher die einfachste Form (6, 3, 90) oder $A = 6$ ist. Hier sind a, a', a'', a''' gleich 1, 2, 3, 6. V enthält die Form (1, 0, 531), V' die folgenden: (4, 1, 133), (4, 3, 135); V'' die folgenden: (9, 0, 59), (9, 3, 60), (9, 6, 63); endlich V''' die folgenden: (36, 3, 15), (36, 9, 17), (36, 15, 21), (36, 21, 27), (36, 27, 35), (36, 33, 45). Aus diesen zwölf Formen sind aber sechs wegzulassen, nämlich aus V'' die zweite und dritte, aus V''' die erste, dritte, vierte und sechste, welche sämtlich abgeleitete Formen sind; von den sechs übrigen findet man, dass sie alle zu verschiedenen Klassen gehören. In der That ist die Anzahl der eigentlich primitiven (positiven) Klassen mit der Determinante -531 gleich 18 und die Anzahl der uneigentlich primitiven (positiven) Klassen mit der Determinante -59 (oder die Anzahl der aus ihnen abgeleiteten Klassen mit der Determinante -531) gleich 3; somit verhält sich jene zu dieser wie 6 zu 1.

256.

Diese Lösung wird durch die folgenden allgemeinen Bemerkungen noch mehr ins Licht treten.

I. Ist die Ordnung O aus einer eigentlich primitiven Ordnung abgeleitet, so geht A^2 in D auf; ist aber O eine uneigentlich primitive oder

eine aus einer uneigentlich primitiven abgeleitete Ordnung, so ist A gerade, D durch $\frac{1}{4}A^2$ teilbar und der Quotient $\equiv 1 \pmod{4}$. Hiernach wird das Quadrat eines jeden Teilers von A entweder in D oder wenigstens in $4D$ aufgehen, und im letzteren Falle wird der Quotient stets $\equiv 1 \pmod{4}$ sein.

II. Geht a^2 in D auf, so werden die sämtlichen Werte des Ausdrucks $\sqrt{D} \pmod{a^2}$, welche zwischen 0 und $a^2 - 1$ liegen, die folgenden sein: $0, a, 2a, \ldots, a^2 - a$, und daher ist a die Anzahl der Formen V. Aber unter diesen werden nur so viele eigentlich primitiv sein, als Zahlen in der Reihe

$$\frac{D}{a^2}, \; \frac{D}{a^2} - 1, \; \frac{D}{a^2} - 4, \; \ldots, \; \frac{D}{a^2} - (a-1)^2$$

vorhanden sind, welche mit a keinen gemeinschaftlichen Teiler haben. Ist $a = 1$, so wird V nur aus der einen Form $(1, 0, -D)$ bestehen, welche stets eigentlich primitiv ist. Ist $a = 2$ oder irgend eine Potenz von 2, so wird die eine Hälfte von jenen a Zahlen gerade, die andere ungerade sein; daher werden in V $\frac{1}{2}a$ eigentlich primitive Formen vorkommen. Ist a irgend eine andere Primzahl p oder die Potenz einer Primzahl, so sind drei Fälle zu unterscheiden, nämlich: Alle jene a Zahlen sind prim zu a und daher sämtliche Formen in V eigentlich primitiv, wenn $\frac{D}{a^2}$ durch p nicht teilbar und gleichzeitig nicht quadratischer Rest von p ist; geht dagegen p in $\frac{D}{a^2}$ auf, so giebt es in V $\frac{(p-1)a}{p}$ eigentlich primitive Formen; ist endlich $\frac{D}{a^2}$ ein durch p nicht teilbarer quadratischer Rest von p, so giebt es in V $\frac{(p-2)a}{p}$ eigentlich primitive Formen. Dies alles lässt sich ohne Schwierigkeit beweisen. Setzt man aber allgemein $a = 2^\nu p^\pi q^\chi r^\rho \ldots$, wo $p, q, r, \ldots$ von einander verschiedene ungerade Primzahlen bezeichnen, so ist die Anzahl der eigentlich primitiven Formen in V gleich $NPQR \ldots$, wo gesetzt werden muss:

$N = 1$ (wenn $\nu = 0$) oder $N = 2^{\nu-1}$ (wenn $\nu > 0$)

$P = p^\pi$ (wenn $\frac{D}{a^2}$ quadratischer Nichtrest von p ist) oder

$P = (p-1)p^{\pi-1}$ (wenn $\frac{D}{a^2}$ durch p teilbar ist) oder

$P = (p-2)p^{\pi-1}$ (wenn $\frac{D}{a^2}$ ein durch p nicht teilbarer quadratischer Rest von p ist),

und $Q, R, \ldots$ sind respective aus $q, r, \ldots$ in derselben Weise zu bestimmen, wie P aus p.

III. Geht a^2 nicht in D auf, so ist $\frac{4D}{a^2}$ eine ganze Zahl und $\equiv 1 \pmod{4}$; die Werte des Ausdrucks $\sqrt{D} \pmod{a^2}$ sind: $\frac{1}{2}a, \frac{3}{2}a, \frac{5}{2}a, \ldots, a^2 - \frac{1}{2}a$; daher

ist die Anzahl der Formen in V gleich a und hiervon werden soviele eigentlich primitiv sein, als es unter den Zahlen

$$\frac{D}{a^2}-\frac{1}{4},\ \frac{D}{a^2}-\frac{9}{4},\ \frac{D}{a^2}-\frac{25}{4},\ldots,\ \frac{D}{a^2}-\left(a-\frac{1}{2}\right)^2$$

zu a prime Zahlen giebt. Sooft $\frac{4D}{a^2}\equiv 1 \pmod{8}$ ist, sind alle diese Zahlen gerade und daher giebt es in V keine eigentlich primitive Form; wenn dagegen $\frac{4D}{a^2}\equiv 5 \pmod{8}$ ist, so sind alle jene Zahlen ungerade, und daher in V alle Formen eigentlich primitiv, falls $a=2$ oder eine Potenz von 2 ist, allgemein aber werden in diesem Falle so viele Formen in V eigentlich primitiv sein, als es unter jenen Zahlen durch keinen ungeraden Primteiler von a teilbare Zahlen giebt. Diese Anzahl ist gleich $NPQR\ldots$, wenn $a=2^\nu p^\pi q^\chi r^\rho\ldots$ ist, wobei $N=2^\nu$ zu setzen ist, die anderen $P, Q, R, \ldots$ aber aus $p, q, r, \ldots$ in derselben Weise herzuleiten sind wie im vorhergehenden Falle.

IV. Auf diese Weise können also die Anzahlen der eigentlich primitiven Formen in $V, V', V'', \ldots$ bestimmt werden; für die Summe aller dieser Anzahlen findet man ohne Schwierigkeit die folgende allgemeine **Regel**: Ist $A=2^\nu\mathfrak{A}^\alpha\mathfrak{B}^\beta\mathfrak{C}^\gamma\ldots$, wo $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$ von einander verschiedene ungerade Primzahlen bezeichnen, so ist die Gesamtanzahl aller eigentlich primitiven Formen in $V, V', V'', \ldots$ gleich $\frac{A\mathfrak{n}\mathfrak{a}\mathfrak{b}\mathfrak{c}\ldots}{2\mathfrak{A}\mathfrak{B}\mathfrak{C}\ldots}$, wo gesetzt werden muss:

$\mathfrak{n}=1$ (wenn $\frac{4D}{A^2}\equiv 1 \pmod{8}$ ist), oder

$\mathfrak{n}=2$ (wenn $\frac{D}{A^2}$ eine ganze Zahl ist) oder

$\mathfrak{n}=3$ (wenn $\frac{4D}{A^2}\equiv 5 \pmod{8}$ ist); ferner

$\mathfrak{a}=\mathfrak{A}$ (wenn $\mathfrak{A}$ in $\frac{4D}{A^2}$ aufgeht) oder

$\mathfrak{a}=\mathfrak{A}\pm 1$ (wenn $\mathfrak{A}$ in $\frac{4D}{A^2}$ nicht aufgeht, wobei das obere oder untere Zeichen zu nehmen ist, je nachdem $\frac{4D}{A^2}$ quadratischer Nichtrest oder Rest von $\mathfrak{A}$ ist);

und $\mathfrak{b}, \mathfrak{c}, \ldots$ aus $\mathfrak{B}, \mathfrak{C}, \ldots$ in derselben Weise abgeleitet werden müssen wie $\mathfrak{a}$ aus $\mathfrak{A}$. Die Kürze gestattet uns nicht, den Beweis hier weitläufiger zu entwickeln.

V. Was nun die Anzahl der **Klassen** anlangt, welche die eigentlich primitiven Formen in $V, V', V'', \ldots$ liefern, so müssen die drei folgenden Fälle unterschieden werden:

Erstens, wenn D eine negative Zahl ist, so bilden die einzelnen eigentlich primitiven Formen in $V, V', \ldots$ je eine besondere Klasse, oder die Anzahl der gesuchten Klassen wird ausgedrückt durch die in der vorigen Bemerkung angegebene Formel, ausgenommen in zwei Fällen, nämlich wenn $\frac{4D}{A^2}$ entweder $= -4$ oder $= -3$ oder wenn D entweder $= -A^2$ oder $= -\frac{3}{4}A^2$ ist. Um diesen Satz zu beweisen, braucht man offenbar nur zu zeigen, dass es nicht möglich sei, dass zwei verschiedene Formen aus $V, V', V'', \ldots$ eigentlich äquivalent sind. Nimmt man daher an, dass (h^2, i, k), (h'^2, i', k') zwei verschiedene eigentlich primitive Formen aus $V, V', V'', \ldots$ seien, welche zu derselben Klasse gehören, und geht die erstere in die letztere über durch die eigentliche Substitution $\alpha, \beta, \gamma, \delta$, so dass man die Gleichungen hat:

$$\alpha\delta - \beta\gamma = 1, \quad h^2\alpha^2 + 2i\alpha\gamma + k\gamma^2 = h'^2, \quad h^2\alpha\beta + i(\alpha\delta + \beta\gamma) + k\gamma\delta = i',$$

so folgt hieraus leicht: erstens, dass γ sicher nicht gleich 0 ist (denn hieraus würde folgen, dass $\alpha = \pm 1$, $h^2 = h'^2$, $i' \equiv i \pmod{h^2}$ ist und daher die gegebenen Formen identisch sind, was der Voraussetzung widerspricht); zweitens, dass γ durch den grössten gemeinschaftlichen Teiler der Zahlen h, h' teilbar ist (denn setzt man diesen Teiler gleich r, so geht derselbe offenbar auch in $2i, 2i'$ auf, ist aber zu k prim; ausserdem geht r^2 in $h^2k - h'^2k' = i^2 - i'^2$ auf, woraus leicht folgt, dass r auch in $i - i'$ aufgeht; man hat aber $\alpha i' - \beta h'^2 = \alpha i + \gamma k$, mithin ist γk und somit auch γ durch r teilbar); drittens, dass $(\alpha h^2 + \gamma i)^2 - D\gamma^2 = h^2h'^2$ ist. Setzt man daher $\alpha h^2 + \gamma i = rp$, $\gamma = rq$, so sind p, q ganze Zahlen, deren letztere nicht gleich 0 ist, und es ist: $p^2 - Dq^2 = \frac{h^2h'^2}{r^2}$. Nun ist aber $\frac{h^2h'^2}{r^2}$ die kleinste gleichzeitig durch h^2 und h'^2 teilbare Zahl und geht daher auch in A^2 und somit auch in $4D$ auf; folglich ist $\frac{4Dr^2}{h^2h'^2}$ eine ganze (negative) Zahl, und setzen wir diese gleich $-e$, so wird $p^2 - Dq^2 = -\frac{4D}{e}$, oder $4 = \left(\frac{2rp}{hh'}\right)^2 + eq^2$. In dieser Gleichung muss der Teil $\left(\frac{2rp}{hh'}\right)^2$ als Quadrat, welches kleiner als 4 ist, notwendig entweder gleich 0 oder gleich 1 sein. Im ersteren Falle ist $eq^2 = 4$ und $D = -\left(\frac{hh'}{rq}\right)^2$, woraus folgt, dass $\frac{4D}{A^2}$ ein mit negativem Vorzeichen behaftetes Quadrat und daher sicher nicht $\equiv 1 \pmod{4}$, also O weder eine uneigentlich primitive noch aus einer uneigentlich primitiven abgeleitete Ordnung ist. Demnach ist $\frac{D}{A^2}$ eine ganze Zahl, woraus leicht folgt, dass e durch 4 teilbar, $q^2 = 1$, $D = -\left(\frac{hh'}{r}\right)^2$ und auch $\frac{A^2}{D}$ eine ganze Zahl ist. Hiernach ist notwendig $D = -A^2$ oder $\frac{D}{A^2} = -1$, welches der

erste Ausnahmefall ist. Im letzteren Falle ist $eq^2 = 3$, also $e = 3$ und $4D = -3\left(\frac{hh'}{r}\right)^2$. Hiernach ist $3\left(\frac{hh'}{rA}\right)^2$ eine ganze Zahl, welche keine andere sein kann als 3, da sie mit einem ganzen Quadrate $\left(\frac{rA}{hh'}\right)^2$ multipliciert die Zahl 3 hervorbringt. Mithin ist $4D = -3A^2$ oder $D = -\frac{3}{4}A^2$, welches der zweite Ausnahmefall ist. In allen übrigen Fällen also werden sämtliche eigentlich primitiven Formen in V, V', V'', ... zu verschiedenen Klassen gehören. — Für die Ausnahmefälle möge es genügen, die Resultate aus einer nicht schwierigen, aber hier der Kürze wegen weggelassenen Untersuchung anzugeben. Im ersten Falle werden nämlich von den eigentlich primitiven Formen in V, V', V'', ... immer je zwei, im zweiten Falle je drei zu derselben Klasse gehören, so dass die Anzahl aller gesuchten Klassen in jenem Fälle die Hälfte, in diesem der dritte Teil des in der vorigen Bemerkung angegebenen Ausdrucks ist.

Zweitens, wenn D eine positive Quadratzahl ist, so werden die einzelnen eigentlich primitiven Formen in V, V', V'', ... ohne Ausnahme je eine besondere Klasse bilden. Denn nimmt man an, dass (h^2, i, k), (h'^2, i', k') zwei solche verschiedene eigentlich äquivalente Formen seien, und geht die erste in die zweite durch die eigentliche Substitution $\alpha, \beta, \gamma, \delta$ über, so werden offenbar alle im vorigen Falle gemachten Schlussfolgerungen, in denen es nicht auf die Voraussetzung, dass D negativ sei, ankam, auch hier gelten. Bezeichnen daher p, q, r hier dasselbe wie dort, so wird auch hier $\frac{4Dr^2}{h^2h'^2}$ eine ganze Zahl sein, aber nicht mehr eine negative, sondern eine positive und überdies quadratische Zahl, und wird diese gleich g^2 gesetzt, so ist $\left(\frac{2rp}{hh'}\right)^2 - g^2q^2 = 4$. Dies ist aber absurd, da die Differenz zweier Quadrate nicht gleich 4 sein kann, wofern nicht das kleinere Quadrat gleich 0 ist. Daher kann die Annahme nicht richtig sein.

Für den **dritten** Fall aber, in welchem D eine positive nichtquadratische Zahl ist, besitzen wir bisher noch keine allgemeine Regel, um die Anzahl der eigentlich primitiven Formen in V, V', V'', ... mit der Anzahl der verschiedenen daraus hervorgehenden Klassen vergleichen zu können. Nur das können wir behaupten, dass diese entweder jener gleich oder ein aliquoter Teil derselben ist; ja wir haben sogar einen eigentümlichen Zusammenhang zwischen dem Quotienten dieser Zahlen und den kleinsten der Gleichung $t^2 - Du^2 = A^2$ genügenden Werten von t, u entdeckt, den hier zu entwickeln zu weit führen würde; ob es aber möglich ist, jenen Quotienten in allen Fällen aus dem blossen Anblick der Zahlen D, A zu erkennen (wie in den vorigen Fällen), darüber können wir nichts sicheres voraussagen. Wir geben hier einige Beispiele, deren Zahl jeder leicht wird vermehren können. Für $D = 13$, $A = 2$ ist die Anzahl der eigentlich primitiven Formen in V, ... gleich 3, welche sämtlich äquivalent

sind oder nur eine einzige Klasse bilden; für $D = 37$, $A = 2$ giebt es auch drei eigentlich primitive Formen in $V, \ldots$, welche zu drei verschiedenen Klassen gehören; für $D = 588$, $A = 7$ hat man acht eigentlich primitive Formen in $V, \ldots$, welche vier Klassen bilden; für $D = 867$, $A = 17$ kommen in $V, \ldots$ achtzehn eigentlich primitive Formen vor, für $D = 1445$, $A = 17$ deren ebensoviele, die aber für jene Determinante in zwei, für diese in sechs Klassen zerfallen.

VI. Aus der Anwendung dieser allgemeinen Theorie auf denjenigen Fall, wo O eine uneigentlich primitive Ordnung ist, folgt, dass sich die Anzahl der in dieser Ordnung enthaltenen Klassen zur Anzahl sämtlicher Klassen in der eigentlich primitiven Ordnung verhält, wie 1 zur Anzahl der verschiedenen eigentlich primitiven Klassen, welche die folgenden drei Formen bilden: $(1, 0, -D)$, $\left(4, 1, \frac{1-D}{4}\right)$ $\left(4, 3, \frac{9-D}{4}\right)$. Und zwar wird hieraus eine einzige Klasse hervorgehen, wenn $D \equiv 1 \pmod{8}$ ist, weil in diesem Falle die zweite und dritte Form uneigentlich primitiv sind; ist aber $D \equiv 5 \pmod{8}$, so werden jene drei Formen sämtlich eigentlich primitiv sein und daher ebenso viele verschiedene Klassen hervorbringen, wenn D negativ ist, den einzigen Fall, wo $D = -3$ ist, ausgenommen, in welchem sie nur eine Klasse bilden; schliesslich gehört der Fall, wo D positiv (von der Form $8n + 5$) ist, zu denen, für welche eine allgemeine Regel bisher noch zu wünschen ist. Das jedoch können wir behaupten, dass jene drei Formen in diesem Falle entweder zu drei verschiedenen Klassen oder zu einer einzigen Klasse, niemals aber zu zwei Klassen gehören. Denn man erkennt leicht, dass, wenn jene Formen $(1, 0, -D)$, $\left(4, 1, \frac{1-D}{4}\right)$, $\left(4, 3, \frac{9-D}{4}\right)$ respective zu den Klassen K, K', K'' gehören, $K + K' = K'$, $K' + K' = K''$ ist, und dass somit, wenn K und K' als identisch angenommen werden, auch K' und K'' identisch sind; ebenso werden, wenn K und K'' als identisch angenommen werden, auch K' und K'' identisch sein; da endlich $K' + K'' = K$ ist, so folgt aus der Annahme, dass K' und K'' identisch seien, auch die Identität von K und K''. Hieraus ergiebt sich, dass entweder alle drei Klassen K, K', K'' verschieden oder alle drei Klassen identisch sind. Z. B. giebt es unterhalb 1000 im Ganzen 125 Zahlen von der Form $8n + 5$, unter denen sich 31 Determinanten befinden, für welche der erstere Fall stattfindet, also die Anzahl der Klassen in der eigentlich primitiven Ordnung dreimal grösser ist als in der uneigentlich primitiven, nämlich 37, 101, 141, 189, 197, 269, 325, 333, 349, 373, 381, 389, 405, 485, 557, 573, 677, 701, 709, 757, 781, 813, 829, 877, 885, 901, 909, 925, 933, 973, 997; für die 94 übrigen gilt der letztere Fall oder für sie ist die Anzahl der Klassen in beiden Ordnungen gleich gross.

VII. Es wird kaum nötig sein zu bemerken, dass nach der vorstehenden Untersuchung nicht allein die Klassenanzahlen in verschiedenen Ordnungen derselben Determinante mit einander verglichen werden können, sondern

dass jene auch auf beliebige verschiedene Determinanten, welche unter sich im quadratischen Verhältnis stehen, anwendbar ist. Bezeichnet nämlich O irgend eine Ordnung der Determinante dm^2, O' eine Ordnung der Determinante dm'^2, so kann O verglichen werden mit der eigentlich primitiven Ordnung mit der Determinante dm^2 und diese mit der Ordnung, welche aus der eigentlich primitiven Ordnung mit der Determinante d abgeleitet ist, oder, was hinsichtlich der Anzahl der Klassen auf dasselbe hinauskommt, mit dieser letzteren Ordnung selbst, und mit eben derselben wird auf gleiche Weise die Ordnung O' verglichen werden können.

Über die Anzahl der ambigen Klassen.

257.

Unter allen Klassen in einer gegebenen Ordnung mit gegebener Determinante erfordern besonders die ambigen Klassen eine ausführlichere Untersuchung, und die Bestimmung der Anzahl dieser Klassen wird uns zu vielem andern den Weg bahnen. Es genügt aber, diese Anzahl bloss in der eigentlich primitiven Ordnung zu bestimmen, da die übrigen Fälle auf diesen leicht zurückgeführt werden können. Diese Aufgabe werden wir in der Weise erledigen, dass wir zuerst zeigen, wie man sämtliche eigentlich primitiven ambigen Formen (A, B, C) mit der gegebenen Determinante D, in denen entweder $B = 0$ oder $B = \frac{1}{2}A$ ist, ermittelt, und sodann, wie man aus der Anzahl dieser die Anzahl aller eigentlich primitiven ambigen Formen mit der Determinante D findet.

I. Man findet offenbar sämtliche eigentlich primitiven Formen $(A, 0, C)$ mit der Determinante D, wenn man für A die einzelnen Teiler von D (sowohl positiv als negativ) nimmt, für welche $C = -\frac{D}{A}$ prim zu A wird. Wenn daher $D = 1$ ist, giebt es zwei derartige Formen $(1, 0, -1)$, $(-1, 0, 1)$; ebenso viele giebt es, wenn $D = -1$ ist, nämlich $(1, 0, 1)$, $(-1, 0, -1)$; ist D eine Primzahl oder die Potenz einer Primzahl (sei es mit positivem, sei es mit negativem Vorzeichen), so giebt es vier: $(1, 0, -D)$, $(-1, 0, D)$, $(D, 0, -1)$, $(-D, 0, 1)$. Allgemein aber giebt es, wenn D durch n verschiedene Primzahlen (zu denen hier auch 2 gerechnet werden muss) teilbar ist, im Ganzen 2^{n+1} derartige Formen. Setzt man nämlich $D = \pm PQR \ldots$, wo $P, Q, R, \ldots$ von einander verschiedene Primzahlen oder Potenzen solcher, deren Anzahl gleich n ist, bezeichnen, so werden die Werte von A die Zahlen $1, P, Q, R, \ldots$ und Producte aus beliebig vielen dieser Zahlen sein; die Anzahl dieser Werte ist nach der Combinationslehre gleich 2^n; dieselbe muss aber verdoppelt werden, da man den einzelnen Werten sowohl das positive wie das negative Vorzeichen beilegen muss.

II. In ähnlicher Weise ergiebt sich, dass alle eigentlich primitiven Formen $(2B, B, C)$ mit der Determinante D erhalten werden, wenn man für B alle Teiler von D (positiv und negativ) nimmt, für welche $C = \frac{1}{2}\left(B - \frac{D}{B}\right)$ eine ganze Zahl und prim zu $2B$ wird. Da somit C notwendig ungerade und daher $C^2 \equiv 1 \pmod{8}$ sein muss, so folgt aus $D = B^2 - 2BC = (B - C)^2 - C^2$, dass D entweder $\equiv 3 \pmod{4}$, wenn B ungerade ist, oder $\equiv 0 \pmod{8}$, wenn B gerade ist; sooft daher D irgend einer der Zahlen 1, 2, 4, 5, 6 nach dem Modul 8 congruent ist, giebt es keine derartigen Formen. Ist $D \equiv 3 \pmod{4}$, so ist C ganz und ungerade, welchen Teiler von D man auch für B nehmen möge; damit aber C mit $2B$ keinen gemeinschaftlichen Teiler habe, muss man B so nehmen, dass $\frac{D}{B}$ zu B prim wird. Hiernach erhält man für $D = -1$ die beiden Formen $(2, 1, 1)$, $(-2, -1, -1)$, und allgemein ist leicht ersichtlich, dass, wenn die Anzahl aller in D aufgehenden Primzahlen gleich n ist, im Ganzen 2^{n+1} Formen entstehen. — Ist D durch 8 teilbar, so wird C eine ganze Zahl, wenn man für B irgend einen geraden Teiler von $\frac{1}{2}D$ nimmt; der andern Bedingung aber, dass $C = \frac{1}{2}B - \frac{D}{2B}$ zu $2B$ prim sein soll, genügt man erstens dadurch, dass man für B alle ungerademal geraden Teiler von D nimmt, für welche $\frac{D}{B}$ mit B keinen gemeinschaftlichen Teiler hat, und deren Anzahl (mit Rücksicht auf die Verschiedenheit der Vorzeichen) gleich 2^{n+1} ist, wenn man annimmt, dass D durch n verschiedene ungerade Primzahlen teilbar sei; zweitens dadurch, dass man für B alle grademal geraden Teiler von $\frac{1}{2}D$ nimmt, für welche $\frac{D}{2B}$ prim zu B wird und deren Anzahl ebenfalls 2^{n+1} ist, so dass man in diesem Falle im Ganzen 2^{n+2} derartige Formen erhält. Setzt man nämlich $D = \pm 2^{\mu} PQR \ldots$, wo μ einen Exponenten bezeichnet, der grösser als 2 ist, und $P, Q, R, \ldots$ verschiedene ungerade Primzahlen oder Potenzen von solchen, deren Anzahl gleich n ist, sind, so können sowohl für $\frac{1}{2}B$ als auch für $\frac{D}{2B}$ die Werte $1, P, Q, R, \ldots$ und die Producte aus beliebig vielen dieser Zahlen sowohl mit positivem als auch mit negativem Vorzeichen genommen werden.

Aus allem diesen folgert man, dass, wenn D durch n verschiedene ungerade Primzahlen teilbar angenommen wird (wo $n = 0$ zu setzen ist, wenn $D = \pm 1$ oder ± 2 oder eine Potenz von 2 ist), die Anzahl aller eigentlich primitiven Formen (A, B, C), in denen B entweder gleich 0 oder gleich $\frac{1}{2}A$ ist, gleich 2^{n+1}, wenn $D \equiv 1$ oder $\equiv 5 \pmod{8}$, gleich 2^{n+2}, wenn $D \equiv 2, 3, 4, 6$ oder $7 \pmod{8}$, endlich gleich 2^{n+3} ist, wenn $D \equiv 0 \pmod{8}$ ist. Vergleicht man diese Zahl mit demjenigen, was wir im Artikel 231 für die Anzahl aller möglichen Charactere der primitiven Formen mit der

Determinante D angegeben haben, so bemerkt man, dass jene in allen Fällen genau doppelt so gross ist als diese. Übrigens ist klar, dass, wenn D negativ ist, es stets unter jenen Formen ebenso viele positive wie negative giebt.

258.

Alle im vorigen Artikel abgeleiteten Formen gehören offenbar zu ambigen Klassen, und umgekehrt muss in jeder ambigen eigentlich primitiven Klasse mit der Determinante D wenigstens eine jener Formen enthalten sein; denn in einer solchen Klasse kommen sicher ambige Formen vor und jeder eigentlich primitiven ambigen Form (a, b, c) mit der Determinante D ist irgend eine der Formen des vorigen Artikels äquivalent, nämlich

$$\text{entweder } \left(a,\ 0,\ -\frac{D}{a}\right) \text{ oder } \left(a,\ \tfrac{1}{2}a,\ \tfrac{1}{4}a-\frac{D}{a}\right),$$

je nachdem b entweder $\equiv 0$ oder $\equiv \frac{1}{2}a \pmod{a}$ ist. Die Aufgabe ist daher darauf zurückgeführt, zu ermitteln, wie viele verschiedene Klassen jene Formen bilden.

Kommt die Form $(a, 0, c)$ unter den Formen des vorigen Artikels vor, so wird die Form $(c, 0, a)$ ebenfalls unter ihnen vorkommen und von jener stets verschieden sein, ausser in dem einen Falle, wo $a = c = \pm 1$ und daher $D = -1$ ist, welchen Fall wir einstweilen unberücksichtigt lassen. Da aber diese Formen offenbar zu derselben Klasse gehören, so braucht man nur eine beizubehalten, und zwar lassen wir diejenige weg, bei welcher das erste Glied grösser ist als das dritte; den Fall, wo $a = -c = \pm 1$ oder $D = 1$ ist, lassen wir ebenfalls noch bei Seite. Auf diese Weise können wir sämtliche Formen $(A, 0, C)$ auf die Hälfte reducieren, indem wir von je zweien stets nur eine beibehalten, und in allen übrigbleibenden ist $A < \sqrt{\pm D}$.

In analoger Weise wird, wenn unter den Formen des vorigen Artikels die Form $(2b, b, c)$ vorkommt, sich unter ihnen auch die Form finden:

$$(4c - 2b,\ 2c - b,\ c) = \left(-\frac{2D}{b}, -\frac{D}{b}, c\right),$$

welche jener eigentlich äquivalent und von ihr verschieden ist, den einen Fall, den wir zurücklegen, ausgenommen, wo $c = b = \pm 1$ oder $D = -1$ ist. Von diesen beiden Formen braucht man nur diejenige beizubehalten, deren erstes Glied kleiner ist, als das erste Glied der andern (an Grösse gleich, dem Vorzeichen nach aber verschieden können sie in diesem Falle nicht sein); daraus geht hervor, dass auch alle Formen $(2B, B, C)$ auf die Hälfte reduciert werden können, indem man von je zweien immer nur eine beibehält, und dass in den übrigbleibenden $B < \frac{D}{B}$ oder $B < \sqrt{\pm D}$ ist. Auf diese Weise bleibt von sämtlichen Formen des vorigen Artikels nur die

Hälfte übrig, deren Gesamtheit wir mit W bezeichnen wollen, und es bleibt nur noch übrig zu zeigen, wieviel verschiedene Klassen aus diesen hervorgehen können. Übrigens ist klar, dass in dem Falle, wo D negativ ist, ebensoviele positive Formen in W enthalten sind wie negative.

I. Ist D negativ, so werden die einzelnen Formen in W zu verschiedenen Klassen gehören. Denn alle Formen $(A, 0, C)$ sind reduciert, ebenso sind alle Formen $(2B, B, C)$ reduciert mit Ausnahme derjenigen, in welchen $C < 2B$ ist. In einer solchen Form aber ist $2C < 2B + C$, daher (weil $B < \frac{D}{B}$ d. i. $B < 2C - B$ und daher $2B < 2C$ oder $B < C$ ist) $2C - 2B < C$ und $C - B < \frac{1}{2} C$, und somit ist $(C, C - B, C)$, welche jener offenbar äquivalent ist, eine reducierte Form. Auf diese Weise hat man ebensoviele reducierte Formen, als Formen in W vorhanden sind, und da man leicht sieht, dass unter jenen weder identische noch entgegengesetzte vorkommen können (ausser in dem Falle, wo $C - B = 0$, in welchem $B = C = \pm 1$ und daher $D = -1$ ist, welchen Fall wir schon zurückgelegt haben), so werden alle Formen zu verschiedenen Klassen gehören. Hieraus folgt, dass die Anzahl aller ambigen eigentlich primitiven Klassen mit der Determinante D der Anzahl der Formen in W oder der Hälfte der Anzahl der Formen des vorigen Artikels gleich ist; in dem ausgeschlossenen Falle $D = -1$ aber findet durch Compensation dasselbe statt, denn man hat zwei Klassen, zu deren einer die Formen $(1, 0, 1)$, $(2, 1, 1)$, zu deren anderer die Formen $(-1, 0, -1)$, $(-2, -1, -1)$ gehören. Allgemein ist also für eine negative Determinante die Anzahl aller ambigen eigentlich primitiven Klassen gleich der Anzahl aller möglichen Charactere der primitiven Formen dieser Determinante; die Anzahl der positiven ambigen eigentlich primitiven Klassen aber ist die Hälfte davon.

II. Ist D eine positive Quadratzahl h^2, so beweist man ohne Schwierigkeit, dass die einzelnen Formen in W zu verschiedenen Klassen gehören, in diesem Falle können wir aber zur Lösung des Problems noch kürzer auf folgende Weise gelangen. Da nach Artikel 210 in jeder ambigen eigentlich primitiven Klasse mit der Determinante h^2, und in keiner andern weiter, eine reducierte Form $(a, h, 0)$ enthalten ist, in welcher a der Wert des Ausdrucks $\sqrt{1}$ (mod. $2h$) ist und zwischen 0 und $2h-1$ incl. liegt, so ist ersichtlich, dass es ebenso viele eigentlich primitive ambige Klassen mit der Determinante h^2 giebt, als jener Ausdruck Werte hat. Aus Artikel 105 aber ergiebt sich leicht, dass die Anzahl dieser Werte gleich 2^n oder 2^{n+1} oder 2^{n+2} ist, je nachdem h entweder ungerade oder ungerademal gerade oder gerademal gerade, d. h. je nachdem $D \equiv 1$ oder $\equiv 4$ oder $\equiv 0$ (mod. 8) ist, wobei n die Anzahl der ungeraden Primteiler von h oder D bezeichnet. Hieraus folgt, dass die Anzahl der ambigen eigentlich primitiven Klassen stets die Hälfte der Anzahl aller im vorigen Artikel abgeleiteten Formen oder gleich der Anzahl der Formen in W oder gleich der Anzahl aller möglichen Charactere ist.

III. Ist D eine positive nichtquadratische Zahl, so leiten wir aus den einzelnen Formen (A, B, C), welche in W enthalten sind, andere (A, B', C') her, indem wir $B' \equiv B$ (mod. A) und zwischen den Grenzen $\sqrt{D}$ und $\sqrt{D} \mp A$ (wo das obere oder untere Zeichen anzuwenden ist, je nachdem A positiv oder negativ ist) und $C' = \frac{B'^2 - D}{A}$ annehmen, und bezeichnen den Complex dieser mit W'. Offenbar sind diese Formen eigentlich primitive ambige Formen mit der Determinante D und alle von einander verschieden; ausserdem aber sind sämtliche Formen reduciert. Denn wenn $A < \sqrt{D}$ ist, so ist offenbar $B' < \sqrt{D}$ und positiv; überdies $B' > \sqrt{D} \mp A$ und daher $A > \sqrt{D} - B'$ und somit A, positiv genommen, sicher zwischen $\sqrt{D} + B'$ und $\sqrt{D} - B'$ gelegen. Wenn aber $A > \sqrt{D}$ ist, so kann nicht $B = 0$ sein (da wir diese Formen verworfen haben), sondern es wird notwendig $B = \frac{1}{2} A$ sein; demnach ist B' an Grösse gleich $\frac{1}{2} A$ aber mit positivem Vorzeichen behaftet (denn da $A < 2\sqrt{D}$, so liegt $\pm \frac{1}{2} A$ zwischen den für B' angegebenen Grenzen und ist B nach dem Modul A congruent, daher $B' = \pm \frac{1}{2} A$), somit $B' < \sqrt{D}$, also $2 B' < \sqrt{D} + B'$ oder $A < \sqrt{D} + B'$; demnach wird $\pm A$ notwendig zwischen den Grenzen $\sqrt{D} + B'$ und $\sqrt{D} - B'$ liegen. Endlich enthält W' sämtliche reducierten eigentlich primitiven ambigen Formen mit der Determinante D; denn wenn (a, b, c) eine solche Form ist, so ist entweder $b \equiv 0$ oder $b \equiv \frac{1}{2} a$ (mod. a). Im ersten Falle kann offenbar nicht $b < a$ und daher auch nicht $a > \sqrt{D}$ sein, weshalb die Form $\left(a, 0, -\frac{D}{a}\right)$ sicher in W und die entsprechende (a, b, c) in W' enthalten ist. Im zweiten Falle ist sicher $a < 2\sqrt{D}$ und daher $\left(a, \frac{1}{2} a, \frac{1}{4} a - \frac{D}{a}\right)$ in W und die entsprechende (a, b, c) in W' enthalten. Hieraus schliesst man, dass die Anzahl der Formen in W gleich ist der Anzahl aller reducierten eigentlich primitiven ambigen Formen mit der Determinante D; da jedoch in den einzelnen ambigen Klassen je zwei reducierte ambige Formen enthalten sind (Artikel 187, 194), so ist die Anzahl aller ambigen eigentlich primitiven Klassen mit der Determinante D gleich der Hälfte der Anzahl der Formen in W oder gleich der Hälfte aller möglichen Charactere.

259.

Die Anzahl der ambigen **uneigentlich** primitiven Klassen mit der gegebenen Determinante D ist der Anzahl der eigentlich primitiven ambigen Klassen mit derselben Determinante stets gleich. Es sei K die Hauptklasse und K', K'', ... die übrigen ambigen eigentlich primitiven Klassen dieser Determinante, ferner L irgend eine ambige uneigentlich primitive Klasse mit derselben Determinante, z. B. diejenige, in welcher die Form $(2, 1, \frac{1}{2} - \frac{1}{2}D)$

vorkommt. Dann wird also aus der Composition der Klasse L mit K die Klasse L selbst hervorgehen; aus der Composition der Klasse L mit K', K'', ... mögen die Klassen L', L'', ... sich ergeben, welche offenbar alle zu derselben Determinante D gehören und uneigentlich primitiv und ambig sind. Offenbar wird daher unser Satz bewiesen sein, wenn gezeigt ist, dass sämtliche Klassen L, L', L'', ... verschieden sind und dass es andere uneigentlich primitive ambige Klassen mit der Determinante D ausser jenen nicht giebt. Zu diesem Zwecke unterscheiden wir folgende Fälle:

I. Wenn die Anzahl der uneigentlich primitiven Klassen der Anzahl der eigentlich primitiven gleich ist, so entsteht eine jede von jenen aus der Composition der Klasse L mit einer bestimmten eigentlich primitiven Klasse, wonach notwendig sämtliche L, L', L'', ... verschieden sind. Bezeichnet aber $\mathfrak{L}$ irgend eine uneigentlich primitive ambige Klasse mit der Determinante D, so giebt es eine eigentlich primitive Klasse $\mathfrak{K}$ von solcher Beschaffenheit, dass $\mathfrak{K} + L = \mathfrak{L}$ ist; ist der Klasse $\mathfrak{K}$ die Klasse $\mathfrak{K}'$ entgegengesetzt, so wird auch (da die Klassen L, $\mathfrak{L}$ sich selbst entgegengesetzt sind), $\mathfrak{K}' + L = \mathfrak{L}$ sein, weshalb notwendig $\mathfrak{K}$ mit $\mathfrak{K}'$ identisch und daher die Klasse ambig ist. Hiernach findet sich $\mathfrak{K}$ unter den Klassen K, K', K'', ... und $\mathfrak{L}$ unter den Klassen L, L', L'', ...

II. Wenn die Anzahl der uneigentlich primitiven Klassen dreimal kleiner ist als die Anzahl der eigentlich primitiven Klassen, so sei H die Klasse, in welcher die Form $\left(4, 1, \frac{1-D}{4}\right)$, H' die Klasse, in welcher die Form $\left(4, 3, \frac{9-D}{4}\right)$ enthalten ist. Dann sind H, H' eigentlich primitiv und sowohl unter sich als von der Hauptklasse K verschieden und ferner $H + H' = K$, $2H = H'$, $2H' = H$, und wenn $\mathfrak{L}$ irgend eine uneigentlich primitive Klasse mit der Determinante D ist, welche aus der Composition der Klasse L mit der eigentlich primitiven Klasse $\mathfrak{K}$ entsteht, so wird auch $\mathfrak{L} = L + \mathfrak{K} + H$ und $\mathfrak{L} = L + \mathfrak{K} + H'$ sein; ausser den drei (eigentlich primitiven und von einander verschiedenen) Klassen $\mathfrak{K}$, $\mathfrak{K} + H$, $\mathfrak{K} + H'$ wird es keine andern weiter geben, welche mit L componiert $\mathfrak{L}$ hervorbringen. Da nun, wenn $\mathfrak{L}$ ambig und $\mathfrak{K}'$ der Klasse $\mathfrak{K}$ entgegengesetzt ist, auch $L + K' = \mathfrak{L}$ ist, so wird notwendig $\mathfrak{K}'$ mit irgend einer jener drei Klassen identisch sein. Ist $\mathfrak{K}' = \mathfrak{K}$, so ist $\mathfrak{K}$ ambig; ist $\mathfrak{K}' = \mathfrak{K} + H$, so wird $K = \mathfrak{K} + \mathfrak{K}' = 2\mathfrak{K} + H = 2(\mathfrak{K} + H')$ und daher $\mathfrak{K} + H'$ ambig; und analog wird, wenn $\mathfrak{K}' = \mathfrak{K} + H'$ ist, $\mathfrak{K} + H$ ambig sein, woraus folgt, dass sich $\mathfrak{L}$ notwendig unter den Klassen L, L', L'', ... vorfindet. Man sieht aber leicht, dass es unter den drei Klassen $\mathfrak{K}$, $\mathfrak{K} + H$, $\mathfrak{K} + H'$ mehrere ambige nicht geben kann; denn wenn $\mathfrak{K}$ und $\mathfrak{K} + H$ beide ambig, also mit den ihnen entgegengesetzten $\mathfrak{K}'$, $\mathfrak{K}' + H'$ resp. identisch wären, so würde $\mathfrak{K} + H = \mathfrak{K} + H'$ sein; derselbe Schluss ergiebt sich aus der Annahme, dass $\mathfrak{K}$ und $\mathfrak{K} + H'$ ambig seien; wenn endlich $\mathfrak{K} + H$, $\mathfrak{K} + H'$ ambig oder mit den zu ihnen entgegengesetzten $\mathfrak{K}' + H'$, $\mathfrak{K}' + H$ identisch wären,

so würde $\mathfrak{K} + H + \mathfrak{K}' + H = \mathfrak{K}' + H' + \mathfrak{K} + H'$ also $2H = 2H'$ oder $H = H'$ sein. Daher giebt es nur eine ambige eigentlich primitive Klasse, welche, mit L zusammengesetzt, $\mathfrak{L}$ hervorbringt, und somit sind L, L', L'', ... sämtlich verschieden.

Die Anzahl der ambigen Klassen in einer abgeleiteten Ordnung ist offenbar gleich der Anzahl der ambigen Klassen in der primitiven Ordnung, aus welcher sie abgeleitet ist, und lässt sich nach dem Vorhergehenden immer bestimmen.

260.

Aufgabe. Die eigentlich primitive Klasse K mit der Determinante D entsteht durch Duplikation der eigentlich primitiven Klasse k mit derselben Determinante; gesucht werden alle gleichartigen Klassen, durch deren Duplikation die Klasse K hervorgeht.

Auflösung. Es sei H die Hauptklasse der Determinante D und H', H'', H''', ... die übrigen ambigen eigentlich primitiven Klassen mit derselben Determinante, und es mögen die Klassen, welche aus der Composition dieser mit k entstehen, nämlich $k + H'$, $k + H''$, $k + H'''$, ..., bezüglich mit k', k'', k''', ... bezeichnet werden. Dann sind alle Klassen k, k', k'', ... eigentlich primitive Klassen der Determinante D und unter einander verschieden; ebenso leicht ist ersichtlich, dass durch Duplikation der einzelnen die Klasse K entsteht. Bezeichnet aber $\mathfrak{K}$ irgend eine eigentlich primitive Klasse mit der Determinante D, welche durch Duplikation die Klasse K hervorbringt, so wird $\mathfrak{K}$ notwendig unter den Klassen k, k', k'', ... enthalten sein. Denn setzt man $\mathfrak{K} = k + \mathfrak{H}$, so dass $\mathfrak{H}$ eine eigentlich primitive Klasse mit der Determinante D ist (Artikel 249), so ist $2k + 2\mathfrak{H} = 2\mathfrak{K} = K = 2k$, woraus leicht folgt, dass $2\mathfrak{H}$ mit der Hauptklasse zusammenfällt, $\mathfrak{H}$ ambig oder unter den Klassen H, H', H'', ... und $\mathfrak{K}$ unter den Klassen k, k', k'', ... enthalten ist. Daher werden diese Klassen die vollständige Lösung der Aufgabe darstellen.

Übrigens ist klar, dass in dem Falle, wo D negativ ist, von den Klassen k, k', k'', ... die Hälfte positiv und die Hälfte negativ ist.

Da somit eine jede eigentlich primitive Klasse mit der Determinante D, welche durch Duplikation irgend einer gleichartigen Klasse entstehen kann, überhaupt durch Duplikation so vieler gleichartigen Klassen hervorgeht, als es ambige eigentlich primitive Klassen mit der Determinante D giebt, so ist klar, dass, wenn die Anzahl sämtlicher eigentlich primitiven Klassen mit der Determinante D gleich r, die Anzahl sämtlicher ambigen eigentlich primitiven Klassen mit dieser Determinante gleich n ist, die Anzahl sämtlicher eigentlich primitiven Klassen mit derselben Determinante, welche durch Duplikation einer gleichartigen Klasse entstehen können, gleich $\frac{r}{n}$ sein wird. Dieselbe Formel ergiebt sich, wenn für eine negative

Determinante die Buchstaben r, n die Anzahl der positiven Klassen bezeichnen und zwar jener die Anzahl aller eigentlich primitiven, dieser nur die Anzahl der ambigen eigentlich primitiven Klassen. So ist z. B. für die Determinante $D = -161$ die Anzahl aller positiven eigentlich primitiven Klassen gleich 16, die Anzahl der ambigen gleicher Art gleich 4, daher muss die Anzahl aller Klassen, welche durch Duplikation irgend einer derselben entstehen können, gleich 4 sein. Und in der That findet man, dass alle in dem Hauptgeschlechte enthaltenen Klassen diese Eigenschaft besitzen; die Hauptklasse (1, 0, 161) nämlich entsteht durch Duplikation der vier ambigen Klassen; (2, 1, 81) durch Duplikation der Klassen (9, 1, 18), (9, —1, 18), (11, 2, 15), (11, —2, 15); (9, 1, 18) durch Duplikation der Klassen (3, 1, 54), (6, 1, 27), (5, —2, 33), (10, 3, 17); schliesslich (9, —1, 18) durch Duplikation der Klassen (3, —1, 54), (6, —1, 27), (5, 2, 33), (10, —3, 17).

Sicher der Hälfte aller für eine gegebene Determinante möglichen Charactere können eigentlich primitive (bei negativer Determinante, positive) Geschlechter nicht entsprechen.

261.

Satz. Der Hälfte aller möglichen Charactere können bei positiver nichtquadratischer Determinante keine eigentlich primitiven, bei negativer Determinante aber keine eigentlich primitiven positiven Geschlechter entsprechen.

Beweis. Es sei m die Anzahl aller eigentlich primitiven (positiven) Geschlechter der Determinante D; k die Anzahl der in den einzelnen Geschlechtern enthaltenen Klassen, so dass km die Anzahl sämtlicher eigentlich primitiven (positiven) Klassen ist, und n die Anzahl aller verschiedenen für diese Determinante möglichen Charactere. Dann ist nach Artikel 258 die Anzahl aller ambigen (positiven) eigentlich primitiven Klassen gleich $\frac{1}{2}n$, und demnach dem vorigen Artikel zufolge die Anzahl aller eigentlich primitiven Klassen, welche durch Duplikation einer gleichartigen Klasse entstehen können, gleich $\frac{2km}{n}$. Nach Artikel 247 gehören aber diese Klassen sämtlich zum Hauptgeschlechte, in welchem k Klassen enthalten sind; wenn daher sämtliche Klassen des Hauptgeschlechts durch Duplikation irgend einer Klasse entstehen können (und dass dies in Wirklichkeit immer stattfindet, wird im Folgenden bewiesen werden), so ist $\frac{2km}{n} = k$, oder $m = \frac{1}{2}n$; sicher aber kann nicht $\frac{2km}{n} > k$ und daher auch nicht $m > \frac{1}{2}n$ sein. Da nun also die Anzahl aller eigentlich primitiven (positiven) Geschlechter

sicher nicht grösser ist als die Hälfte aller möglichen Charactere, so können mindestens der Hälfte dieser derartige Geschlechter nicht entsprechen.

Übrigens muss man wohl beachten, dass hieraus noch nicht folgt, dass der Hälfte aller möglichen Charactere in Wirklichkeit eigentlich primitive (positive) Geschlechter entsprechen, vielmehr wird die Richtigkeit dieses höchst wichtigen Satzes sich weiter unten erst aus den verborgensten Eigenschaften der Zahlen ableiten lassen.

Da für eine negative Determinante immer ebensoviele negativen Geschlechter existieren wie positive, so können offenbar von allen möglichen Characteren nicht mehr als die Hälfte eigentlich primitiven negativen Geschlechtern zugehören, worüber wir ebenso wie über die uneigentlich primitiven Geschlechter weiter unten sprechen werden. Endlich bemerken wir, dass sich der Satz auf positive quadratische Determinanten nicht erstreckt, vielmehr ist ohne Weiteres ersichtlich, dass bei denselben den einzelnen möglichen Characteren in Wirklichkeit auch Geschlechter entsprechen.

Zweiter Beweis des Fundamentalsatzes und der übrigen auf die Reste -1, $+2$, -2 sich beziehenden Sätze.

262.

In dem Falle also, wo für eine gegebene nichtquadratische Determinante D nur zwei verschiedene Charactere möglich sind, wird nur einem einzigen ein eigentlich primitives (positives) Geschlecht entsprechen (welches kein anderes sein kann, als das Hauptgeschlecht), während der andere keiner eigentlich primitiven positiven Form jener Determinante zukommt. Dies ist der Fall für die Determinanten -1, 2, -2, -4, für die positiv genommenen Primzahlen von der Form $4n+1$, für die negativ genommenen Primzahlen von der Form $4n+3$, endlich für alle positiv genommenen ungeraden Potenzen der Primzahlen von der Form $4n+1$ und für die Potenzen der Primzahlen von der Form $4n+3$, und zwar dieselben positiv oder negativ genommen, je nachdem die Exponenten gerade oder ungerade sind. Aus diesem Princip können wir eine **neue Methode** ableiten, nicht nur **um das Fundamentaltheorem,** sondern auch um alle übrigen auf die Reste -1, $+2$, -2 sich beziehenden Sätze des vorigen Abschnittes **zu beweisen,** eine Methode, welche von den im vorigen Abschnitte angewandten Methoden vollständig verschieden ist und an Eleganz hinter diesen keineswegs zurückstehen dürfte. Die Determinante -4 aber und diejenigen Determinanten, welche Potenzen von Primzahlen sind, werden wir, da sie nichts Neues lehren, übergehen.

Für die Determinante -1 giebt es also keine positive Form, deren Character 3, 4 ist; für die Determinante $+2$ überhaupt keine Form, deren Character 3 u. 5, 8 ist; für die Determinante -2 kommt keiner positiven Form der Character 5 u. 7, 8 zu; für die Determinante $+p$, falls p eine

Primzahl von der Form $4n+1$, oder für die Determinante $-p$, falls p eine Primzahl von der Form $4n+3$ ist, kommt keiner eigentlich primitiven (im letzteren Falle positiven) Form der Character Np zu. Hiernach beweisen wir die Sätze des vorigen Abschnitts in folgender Weise:

I. Es ist -1 Nichtrest einer jeden (positiven) Zahl von der Form $4n+3$. Denn wenn -1 Rest einer solchen Zahl A wäre, so würde, wenn man $-1 = B^2 - AC$ setzt, (A, B, C) eine positive Form mit der Determinante -1 sein, deren Character 3, 4 wäre.

II. Es ist -1 Rest jeder Primzahl p von der Form $4n+1$. Denn der Character der Form $(-1, 0, p)$ sowie aller eigentlich primitiven Formen mit der Determinante p ist Rp; demnach -1 Rest von p.

III. Sowohl $+2$ als auch -2 ist Rest einer jeden Primzahl p von der Form $8n+1$. Denn es sind entweder die Formen $\left(8, 1, \frac{1-p}{8}\right)$, $\left(-8, 1, \frac{p-1}{8}\right)$ oder die folgenden $\left(8, 3, \frac{9-p}{8}\right)$, $\left(-8, 3, \frac{p-9}{8}\right)$ eigentlich primitiv (je nachdem n ungerade oder gerade ist) und daher ist ihr Character Rp. Hiernach ist $+8Rp$ und $-8Rp$, daher auch $2Rp$, $-2Rp$.

IV. Es ist $+2$ Nichtrest einer jeden Zahl von der Form $8n+3$ oder $8n+5$. Denn wenn $+2$ Rest einer solchen Zahl A wäre, so würde es eine Form (A, B, C) mit der Determinante $+2$ geben, deren Character 3 u. 5, 8 wäre.

V. Ebenso ist -2 Nichtrest jeder Zahl von der Form $8n+5$ oder $8n+7$, denn sonst würde es eine Form (A, B, C) mit der Determinante -2 geben, deren Character 5 u. 7, 8 wäre.

VI. Es ist -2 Rest jeder Primzahl p von der Form $8n+3$. Diesen Satz kann man auf doppelte Weise beweisen. Erstens: Da nach IV: $+2Np$ und nach I: $-1Np$ ist, so ist notwendig $-2Rp$. Der zweite Beweis gründet sich auf die Betrachtung der Determinante $+2p$, für welche vier Charactere möglich sind, nämlich Rp, 1 u. 3, 8; Rp, 5 u. 7, 8; Np, 1 u. 3, 8; Np, 5 u. 7, 8, und von diesen werden mindestens zweien keine Geschlechter entsprechen. Nun kommt der Form $(1, 0, 2p)$ der erste, der Form $(-1, 0, 2p)$ der vierte Character zu, daher ist der zweite und dritte Character zu verwerfen. Da nun der Character der Form $(p, 0, -2)$ in Bezug auf die Zahl 8 1 u. 3, 8 ist, so kann ihr Character in Bezug auf p kein anderer sein als Rp, daher ist $-2Rp$.

VII. Es ist $+2$ Rest jeder Primzahl p von der Form $8n+7$, was man ebenfalls auf doppelte Weise beweisen kann. Erstens: Da nach I und V: $-1Np$, $-2Np$ ist, so wird $+2Rp$. Zweitens: Da entweder $\left(8, 1, \frac{1+p}{8}\right)$ oder $\left(8, 3, \frac{9+p}{8}\right)$ eine eigentlich primitive Form mit der

Determinante $-p$ ist (je nachdem n gerade oder ungerade ist), so ist ihr Character Rp und daher ist $8Rp$ und $2Rp$.

VIII. Jede beliebige Primzahl p von der Form $4n+1$ ist Nichtrest von jeder ungeraden Zahl q, welche Nichtrest von p ist. Denn wäre p Rest von q, so würde es offenbar eine eigentlich primitive Form mit der Determinante p geben, deren Character Np wäre.

IX. Ebenso ist, wenn irgend eine ungerade Zahl q Nichtrest der Primzahl p von der Form $4n+3$ ist, $-p$ Nichtrest von q; denn sonst würde es eine positive eigentlich primitive Form mit der Determinante $-p$ geben, deren Character Np wäre.

X. Jede Primzahl p von der Form $4n+1$ ist Rest jeder andern Primzahl q, welche Rest von p ist. Wenn auch q von der Form $4n+1$ ist, so folgt dies unmittelbar aus VIII; ist aber q von der Form $4n+3$, so wird (wegen II) auch $-q$ Rest von p und daher pRq (nach IX).

XI. Wenn irgend eine Primzahl q Rest einer andern Primzahl p von der Form $4n+3$ ist, so ist $-p$ Rest von q. Ist nämlich q von der Form $4n+1$, so folgt aus VIII: pRq und daher nach II: $-pRq$; der Fall aber, wo auch q von der Form $4n+3$ ist, entzieht sich dieser Methode, kann jedoch leicht durch Betrachtung der Determinante $+pq$ erledigt werden. Da nämlich zweien von den vier für diese Determinante möglichen Characteren Rp, Rq; Rp, Nq; Np, Rq; Np, Nq keine Geschlechter entsprechen können, und die Charactere der Formen $(1, 0, -pq)$, $(-1, 0, pq)$ respective der erste und vierte sind, so kann der zweite und dritte Character keiner eigentlich primitiven Form mit der Determinante pq zukommen. Da nun der Character der Form $(q, 0, -p)$ in Bezug auf die Zahl p nach Voraussetzung Rp ist, so muss der Character derselben Form in Bezug auf die Zahl q Rq sein, und daher ist $-pRq$.

Nimmt man in den Sätzen VIII und IX an, dass q eine Primzahl bezeichnet, so stellen dieselben in Verbindung mit den Sätzen X und XI das Fundamentaltheorem des vorigen Abschnitts dar.

Es wird diejenige Hälfte der Charactere, denen Geschlechter nicht entsprechen können, näher bestimmt.

263.

Nachdem wir das Fundamentaltheorem von Neuem bewiesen haben, werden wir zeigen, wie man diejenige Hälfte der Charactere, denen keine eigentlich primitiven (positiven) Formen entsprechen können, für irgend eine gegebene nichtquadratische Determinante erkennt, und zwar werden wir diese Aufgabe um so kürzer erledigen können, da das Fundament derselben bereits in der Untersuchung der Artikel 147—150 enthalten ist. Es sei e^2 das grösste Quadrat, welches in der gegebenen Determinante D aufgeht,

und $D = D'e^2$, so dass D' keinen quadratischen Factor enthält; ferner seien $a, b, c, \ldots$ sämtliche ungeraden Primteiler von D' und daher D' abgesehen vom Vorzeichen entweder das Product aus diesen Zahlen oder das Doppelte dieses Productes. Es bezeichne ferner Ω den Complex der Specialcharactere $Na, Nb, Nc, \ldots$, und zwar allein diesen, wenn $D' \equiv 1$ (mod. 4) ist, dagegen nach Hinzufügung des Characters 3, 4, wenn $D' \equiv 3$ und e ungerade oder ungerademal gerade ist; nach Hinzufügung der Charactere 3, 8 und 7, 8, wenn $D' \equiv 3$ und e gerademal gerade ist, nach Hinzufügung entweder des Characters 3 u. 5, 8 oder der beiden 3, 8 und 5, 8, wenn $D' \equiv 2$ (mod. 8) und e entweder ungerade oder gerade ist, endlich nach Hinzufügung entweder des Characters 5 u. 7, 8 oder der beiden 5, 8 und 7, 8, wenn $D' \equiv 6$ (mod. 8) und e entweder ungerade oder gerade ist. Ist dies in dieser Weise geschehen, so werden allen Totalcharacteren, in welchen eine ungerade Anzahl von Specialcharacteren Ω enthalten ist, keine eigentlich primitiven (positiven) Geschlechter mit der Determinante D entsprechen können. In allen übrigen Fällen haben die Specialcharactere, welche die Beziehung zu den in D' nicht aufgehenden Primteilern von D ausdrücken, keinen Einfluss auf die Möglichkeit oder Unmöglchkeit der Geschlechter. — Aus der Combinationslehre aber erkennt man leicht, dass auf diese Weise wirklich die Hälfte aller möglichen Totalcharactere ausgeschlossen wird.

Der Beweis für die Richtigkeit dieser Vorschriften wird in der folgenden Weise geführt. Aus den Prinzipien des vorigen Abschnittes oder aus den im vorigen Artikel von Neuem bewiesenen Sätzen leitet man ohne Schwierigkeit ab, dass, wenn p eine in D nicht aufgehende (ungerade positive) Primzahl ist, welcher irgend einer von den weggelassenen Characteren zukommt, D' eine ungerade Anzahl von Factoren, welche Nichtreste von p sind, enthält und daher D' und somit auch D Nichtrest von p ist. Ferner ist leicht ersichtlich, dass das Product aus beliebig vielen ungeraden zu D primen Zahlen, deren keiner irgend einer der weggelassenen Charactere zukommt, auch mit einem solchen Character nicht verträglich sein kann; hieraus ist umgekehrt klar, dass jede ungerade positive zu D prime Zahl, welcher irgend einer der verworfenen Charactere zugehört, sicher irgend einen Primfactor von derselben Beschaffenheit enthält, und daher D Nichtrest derselben ist. Wenn es daher eine eigentlich primitive (positive) Form mit der Determinante D gäbe, welche einem der verworfenen Charactere entspricht, so würde D Nichtrest von einer jeden durch eine solche Form darstellbaren, positiven ungeraden, zu D primen Zahl sein, was offenbar mit dem Satze des Artikels 154 nicht verträglich ist.

Als Beispiele können die in den Artikeln 231, 232 angegebenen Klassifikationen verglichen werden, deren Anzahl jeder nach Belieben vermehren kann.

264.

Auf diese Weise zerfallen also für irgend eine gegebene nichtquadratische Determinante sämtliche möglichen Charactere in zwei Arten P, Q von der

Beschaffenheit, dass keinem der Charactere Q eine eigentlich primitive (positive) Form entsprechen kann, während nichts im Wege steht, soweit wir bisher es wissen, dass die andern P zu derartigen Formen gehören. In Betreff dieser Arten von Characteren möge insbesondere der folgende Satz angeführt werden, der aus der Erklärung derselben leicht sich ergiebt: Wenn ein Character aus P mit einem Character aus Q zusammengesetzt wird (nach Art des Artikels 246, gerade so als ob auch diesem ein Geschlecht entspräche), so ergiebt sich ein Character aus Q; wenn dagegen zwei Charactere aus P oder zwei aus Q zusammengesetzt werden, so gehört der sich ergebende Character zu P. Mit Hülfe dieses Satzes kann auch für negative und uneigentlich primitive Geschlechter die Hälfte der möglichen Charactere in folgender Weise ausgeschlossen werden.

I. Für eine negative Determinante D werden die negativen Geschlechter den positiven in dieser Beziehung vollständig entgegengesetzt sein, es wird nämlich keiner der Charactere P zu einem eigentlich primitiven negativen Geschlechte gehören, vielmehr werden diese Geschlechter sämtlich Charactere aus Q haben. Denn wenn $D' \equiv 1 \pmod{4}$ ist, so ist $-D'$ eine positive Zahl von der Form $4n+3$ und daher giebt es unter $a, b, c, \ldots$ eine ungerade Anzahl von Zahlen von der Form $4n+3$, von deren jeder -1 Nichtrest ist, woraus hervorgeht, dass in den Totalcharacter der Form $(-1, 0, D)$ in diesem Falle eine ungerade Anzahl von Specialcharacteren aus Ω eingeht, oder dass derselbe zu Q gehört. Ist $D' \equiv 3 \pmod{4}$, so giebt ist unter den Zahlen $a, b, c, \ldots$ entweder keine Zahl von der Form $4n+3$, oder zwei, oder vier, u. s. w.; da aber in diesem Falle entweder 3, 4 oder 3, 8 oder 7, 8 unter den Specialcharacteren der Form $(-1, 0, D)$ vorkommt, so ist klar, dass der Totalcharacter dieser Form auch hier zu Q gehört. Denselben Schluss erhält man ebenso leicht in den übrigen Fällen, so dass die negative Form $(-1, 0, D)$ immer einen Character aus Q hat. Aber da diese Form, mit irgend einer andern negativen eigentlich primitiven Form mit derselben Determinante componiert, eine positive Form der gleichen Art hervorbringt, so sieht man leicht, dass keine negative eigentlich primitive Form einen Character aus P haben kann.

II. Für uneigentlich primitive (positive) Geschlechter beweist man in ähnlicher Weise, dass sich die Sache entweder in derselben oder in entgegengesetzter Weise verhält wie bei eigentlich primitiven, je nachdem $D \equiv 1$ oder $\equiv 5 \pmod{8}$ ist. Denn in dem ersten Falle ist auch $D' \equiv 1 \pmod{8}$, woraus leicht folgt, dass es unter den Zahlen $a, b, c, \ldots$ entweder keine Zahl von der Form $8n+3$ und $8n+5$ giebt, oder zwei oder vier, u. s. w. (denn das Product aus beliebig vielen ungeraden Zahlen, unter denen die Zahlen von der Form $8n+3$ und $8n+5$ zusammen in ungerader Anzahl vertreten sind, wird immer entweder $\equiv 3$ oder $\equiv 5 \pmod{8}$, das Product aus allen Zahlen $a, b, c, \ldots$ muss aber entweder D' oder $-D'$ gleich sein). Hieraus geht hervor, dass der Totalcharacter der Form $\left(2, 1, \frac{1-D}{2}\right)$

entweder keinen Specialcharacter aus Ω oder deren zwei oder vier, u. s. w., enthält und daher zu P gehört. Da nun jede uneigentlich primitive (positive) Form mit der Determinante D als zusammengesetzt betrachtet werden kann aus $\left(2, 1, \frac{1-D}{2}\right)$ und einer eigentlich primitiven (positiven) Form derselben Determinante, so ist ersichtlich, dass keine uneigentlich primitive (positive) Form in diesem Falle einen Character aus Q haben kann. Im zweiten Falle, wo $D \equiv 5$ (mol. 8) ist, ist alles umgekehrt; es wird nämlich D', welches ebenfalls $\equiv 5$ (mod. 8) ist, sicher eine ungerade Anzahl von Factoren von der Form $8n+3$ und $8n+5$ enthalten, woraus folgt, dass der Character der Form $\left(2, 1, \frac{1-D}{2}\right)$ und hiernach auch der Character jeder uneigentlich primitiven (positiven) Form mit der Determinante D zu Q gehört und daher keinem der Charactere P ein uneigentlich primitives positives Geschlecht entsprechen kann.

III. Endlich sind für eine negative Determinante die negativen uneigentlich primitiven Geschlechter wiederum den uneigentlich primitiven positiven Geschlechtern entgegengesetzt; jene können nämlich nicht einen Character aus P oder aus Q haben, je nachdem $D \equiv 1$ oder $\equiv 5$ (mod. 8) oder je nachdem $-D$ von der Form $8n+7$ oder $8n+3$ ist. Dies leitet man ohne Schwierigkeit daraus her, dass aus der Composition der Form $(-1, 0, D)$, deren Character aus Q ist, mit negativen uneigentlich primitiven Formen mit derselben Determinante positive uneigentlich primitive Formen hervorgehen und daher, wenn von diesen die Charactere Q ausgeschlossen sind, von jenen notwendig die Charactere P ausgeschlossen werden müssen, und umgekehrt.

Besondere Methode, Primzahlen in zwei Quadrate zu zerlegen.

265.

Aus den Untersuchungen der Artikel 257, 258 über die Anzahl der ambigen Klassen, auf welchen alles Vorhergehende aufgebaut ist, lassen sich noch viele andere der Beachtung werte Folgerungen ziehen, die wir der Kürze wegen unterdrücken müssen; indessen können wir die folgende, durch ihre Eleganz ausgezeichnete nicht übergehen. Wir haben gezeigt, dass es für eine positive Determinante p, welche eine Primzahl von der Form $4n+1$ ist, nur eine einzige ambige eigentlich primitive Klasse giebt; demnach sind alle ambigen eigentlich primitiven Klassen mit einer solchen Determinante einander eigentlich äquivalent. Wenn daher b die grösste positive ganze Zahl, welche kleiner als $\sqrt{p}$ ist, und $p - b^2 = a'$ ist, so werden die Formen $(1, b, -a')$, $(-1, b, a')$ eigentlich äquivalent und

daher, da offenbar beide reducierte Formen sind, die eine in der Periode der andern enthalten sein. Legt man der ersten Form in ihrer Periode den Index 0 bei, so wird der Index der zweiten notwendig ungerade sein (da die ersten Glieder dieser beiden Formen entgegengesetzte Zeichen haben); derselbe möge daher gleich $2m+1$ gesetzt werden. Ferner sieht man leicht, dass, wenn die Formen mit den Indices 1, 2, 3, ... bezüglich

$$(-a', b', a''),\quad (a'', b'', -a'''),\quad (-a''', b''', a''''), \ldots$$

sind, den Indices $2m$, $2m-1$, $2m-2$, $2m-3$, ... die Formen entsprechen werden:

$$(a', b, -1),\quad (-a'', b', a'),\quad (a''', b'', -a''),\quad (-a'''', b''', a'''), \ldots$$

Hieraus folgt, dass, wenn die Form vom Index m gleich (A, B, C) ist, dieselbe auch gleich $(-C, B, -A)$ und daher $C = -A$ und $p = B^2 + A^2$ ist. Daher lässt sich jede Primzahl von der Form $4n+1$ in zwei Quadrate zerlegen (welche Zerlegung wir oben im Artikel 182 aus ganz verschiedenen Prinzipien abgeleitet haben), und zu einer solchen Zerlegung gelangen wir durch eine höchst einfache und durchaus gleichförmige Methode, nämlich durch Entwicklung der Periode der reducierten Form, deren Determinante jene Primzahl und deren erstes Glied 1 ist, bis zu einer Form, deren äussere Glieder der Grösse nach gleich, dem Vorzeichen nach entgegengesetzt sind. So hat man z. B. für $p = 233$: $(1, 15, -8)$, $(-8, 9, 19)$, $(19, 10, -7)$, $(-7, 11, 16)$, $(16, 5, -13)$, $(-13, 8, 13)$ und $233 = 64 + 169$. Übrigens ist klar, dass A notwendig ungerade (da ja $(A, B, -A)$ eine eigentlich primitive Form sein muss) und somit B gerade wird. — Da für eine positive Determinante p, welche eine Primzahl von der Form $4n+1$ ist, auch in der uneigentlich primitiven Ordnung nur eine einzige ambige Klasse enthalten ist, so ist ersichtlich, dass, wenn g die grösste ungerade Zahl, welcher kleiner als $\sqrt{p}$ ist, und $p - g^2 = 4h$ ist, die reducierten uneigentlich primitiven Formen $(2, g, -2h)$, $(-2, g, 2h)$ eigentlich äquivalent sind und daher die eine in der Periode der andern enthalten ist. Hieraus folgt durch Schlüsse, welche den vorstehenden ganz analog sind, dass sich in der Periode der Form $(2, g, -2h)$ eine Form findet, deren äussere Glieder der Grösse nach gleich sind, aber entgegengesetzte Vorzeichen haben, so dass die Zerlegung der Zahl p in zwei Quadrate auch hieraus abgeleitet werden kann. Offenbar aber werden die äusseren Glieder dieser Form gerade, das mittlere ungerade sein, und da bekanntlich eine Primzahl nur auf eine Weise in zwei Quadrate zerlegt werden kann, so wird die nach dieser letzteren Methode gefundene Form entweder $(B, \pm A, -B)$ oder $(-B, \pm A, B)$ sein. So erhält man in unserm Beispiel für $p = 233$: $(2, 15, -4)$, $(-4, 13, 16)$, $(16, 3, -14)$, $(-14, 11, 8)$, $(8, 13, -8)$ und $233 = 64 + 169$, wie oben.

Digression, enthaltend eine Untersuchung über ternäre Formen.

266.

Bisher haben wir unsere Untersuchung auf solche Functionen zweiten Grades beschränkt, welche zwei Unbestimmte enthalten, und es war daher nicht nötig, ihnen eine besondere Benennung beizulegen. Offenbar aber können wir diesen Gegenstand als einen sehr speciellen Abschnitt der allgemeinsten Untersuchung über die algebraischen rationalen ganzen **homogenen** Functionen mehrerer Unbestimmten und von mehreren Dimensionen betrachten und derartige Functionen nach der Anzahl der Dimensionen in Formen zweiten, dritten, vierten u. s. w. Grades, nach der Anzahl der Unbestimmten aber in binäre, ternäre, quaternäre u. s. w. Formen passend unterscheiden. Die bisher einfach so genannten Formen sind daher binäre Formen zweiten Grades, derartige Functionen aber wie

$$Ax^2 + 2Bxy + Cy^2 + 2Dxz + 2Eyz + Fz^2$$

(wo A, B, C, D, E, F gegebene ganze Zahlen bedeuten) heissen ternäre Formen zweiten Grades u. s. w. Zunächst zwar ist der gegenwärtige Abschnitt bloss den binären Formen zweiten Grades gewidmet; da jedoch mehrere auf diese bezügliche Wahrheiten, und zwar die schönsten, noch übrig sind, deren eigentliche Quelle in der Theorie der ternären Formen zweiten Grades zu suchen ist, so wollen wir hier eine kurze Digression über diese Theorie einschalten, in der wir aus ihren ersten Elementen das anführen wollen, was zur Vervollkommnung der Theorie der binären Formen notwendig ist, und hoffen wir, dass dies den Geometern angenehmer sein wird, als wenn wir jene Wahrheiten entweder unterdrückten oder durch weniger natürliche Methoden ableiteten. Eine genauere Untersuchung über diesen sehr wichtigen Gegenstand müssen wir uns aber für eine andere Gelegenheit vorbehalten, einmal weil die Reichhaltigkeit desselben die Grenzen dieses Werkes schon jetzt weit überschreiten würde, sodann weil Hoffnung vorhanden ist, dass derselbe in Zukunft noch durch ansehnliche Erweiterungen werde bereichert werden. Die quaternären, quinären u. s. w. Formen zweiten Grades sowohl wie auch die Formen höherer Grade schliessen wir wenigstens an dieser Stelle von der Betrachtung gänzlich aus*) und begnügen uns, dieses sehr weite Gebiet der Aufmerksamkeit der Geometer empfohlen zu haben, da sie darin einen ungeheuren Stoff zur Übung ihrer Kräfte und zur Bereicherung der höheren Arithmetik durch hervorragende Erweiterungen finden werden.

---

*) Aus diesem Grunde sind im Folgenden immer binäre oder ternäre Formen zweiten Grades zu verstehen, wenn von solchen Formen schlechthin die Rede ist.

267.

Es wird zur grösseren Deutlichkeit viel beitragen, wenn wir zwischen den drei in die ternäre Form eingehenden Unbestimmten ebenso wie bei den binären Formen eine bestimmte Reihenfolge festsetzen, so dass die erste, zweite und dritte Unbestimmte von einander unterschieden werden. Bei der Aufstellung der einzelnen Teile der Form werden wir ferner immer eine solche Anordnung beobachten, dass derjenige Teil, welcher das Quadrat der ersten Unbestimmten enthält, die erste Stelle erhält, sodann diejenigen Teile, welche das Quadrat der zweiten, das Quadrat der dritten Unbestimmten, das doppelte Product aus der zweiten und dritten, das doppelte Product aus der ersten und dritten, das doppelte Product aus der ersten und zweiten Unbestimmten enthalten, der Reihe nach folgen. Schliesslich werden wir die bestimmten ganzen Zahlen, mit denen diese Quadrate und doppelten Producte multipliciert sind, in ebenderselben Reihenfolge den ersten, zweiten, dritten, vierten, fünften, sechsten Coefficienten nennen. So wird

$$ax^2 + a'x'^2 + a''x''^2 + 2bx'x'' + 2b'xx'' + 2b''xx'$$

eine richtig geordnete ternäre Form sein, deren erste Unbestimmte x, deren zweite x', dritte x'', deren erster Coefficient a, u. s. w., vierter b, u. s. w. ist. Da es aber zur Kürze viel beiträgt, wenn wir nicht stets die Unbestimmten der ternären Form mit besonderen Buchstaben zu bezeichnen brauchen, so werden wir dieselbe Form, sofern wir nicht auf die Unbestimmten Rücksicht nehmen, auch auf die folgende Weise bezeichnen:

$$\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}.$$

Setzt man

$$b^2 - a'a'' = A, \quad b'^2 - aa'' = A', \quad b''^2 - aa' = A''$$
$$ab - b'b'' = B, \quad a'b' - bb'' = B', \quad a''b'' - bb' = B'',$$

so entsteht eine andere Form

$$\begin{pmatrix} A, & A', & A'' \\ B, & B', & B'' \end{pmatrix} = F,$$

welche wir der Form

$$\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix} = f$$

adjungiert nennen werden. Hieraus findet man wieder, wenn man der Kürze wegen die Zahl

$$ab^2 + a'b'^2 + a''b''^2 - aa'a'' - 2bb'b'' = D$$

setzt:

$$B^2 - A'A'' = aD, \quad B'^2 - AA'' = a'D, \quad B''^2 - AA' = a''D,$$
$$AB - B'B'' = bD, \quad A'B' - BB'' = b'D, \quad A''B'' - BB' = b''D,$$

woraus hervorgeht, dass der Form F die Form

$$\begin{pmatrix} aD, & a'D, & a''D \\ bD, & b'D, & b''D \end{pmatrix}$$

adjungiert ist. Die Zahl D, von deren Beschaffenheit die Eigenschaften der ternären Form f hauptsächlich abhängen, werden wir **die Determinante dieser Form** nennen. Auf diese Weise wird die Determinante der Form F gleich D^2 oder gleich dem Quadrate der Determinante der Form f, welcher sie adjungiert ist.

So ist z. B. der ternären Form $\begin{pmatrix} 29, & 13, & 9 \\ 7, & -1, & 14 \end{pmatrix}$ die Form $\begin{pmatrix} -68, & -260, & -181 \\ 217, & -111, & 133 \end{pmatrix}$ adjungiert und die Determinante beider gleich 1.

Die ternären Formen mit der Determinante 0 werden von der nachfolgenden Untersuchung gänzlich ausgeschlossen, da sie, wie in der bei anderer Gelegenheit ausführlicher zu behandelnden Theorie der ternären Formen gezeigt werden wird, nur dem Anblick nach ternäre Formen, in Wirklichkeit aber binären Formen äquivalent sind.

268.

Wenn irgend eine ternäre Form f mit der Determinante D, deren Unbestimmten x, x', x'' (nämlich die erste gleich x, u. s. w.) sind, in die ternäre Form g mit der Determinante E, deren Unbestimmten y, y', y'' sind, durch eine Substitution von der Form

$$\begin{aligned} x &= \alpha y + \beta y' + \gamma y'' \\ x' &= \alpha' y + \beta' y' + \gamma' y'' \\ x'' &= \alpha'' y + \beta'' y' + \gamma'' y'' \end{aligned}$$

übergeht, wo die neun Coefficienten $\alpha, \beta, \ldots$ sämtlich als ganze Zahlen vorausgesetzt werden, so werden wir der Kürze wegen mit Weglassung der Unbestimmten einfach sagen, dass f in g durch die Substitution (S)

$$\begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{matrix}$$

übergehe und dass f die Form g enthalte oder g unter f enthalten sei. Aus einer solchen Voraussetzung ergeben sich daher unmittelbar sechs Gleichungen für die sechs Coefficienten in g, die hierherzusetzen nicht nötig ist; aus diesen erhält man aber durch eine leichte Rechnung die folgenden Schlüsse:

I. Setzt man der Kürze wegen die Zahl

$$\alpha\beta'\gamma'' + \beta\gamma'\alpha'' + \gamma\alpha'\beta'' - \gamma\beta'\alpha'' - \alpha\gamma'\beta'' - \beta\alpha'\gamma'' = k,$$

so findet man nach den gehörigen Reductionen die Gleichung $E = k^2 D$, woraus hervorgeht, dass E durch D teilbar und der Quotient ein Quadrat

ist. Es ist daher klar, dass die Zahl k für die Transformationen ternärer Formen etwas ähnliches ist, wie die Zahl $\alpha\delta - \beta\gamma$ im Artikel 157 für die Transformationen der binären Formen, nämlich die Quadratwurzel aus dem Quotienten der Determinanten, wonach man vermuten könnte, dass die Verschiedenheit des Vorzeichens von k auch hier einen wesentlichen Unterschied zwischen den Transformationen und dem Eigentlich- oder Uneigentlich-Enthaltensein der einen Form in der andern begründe. Betrachtet man aber die Sache näher, so sieht man, dass f auch durch die folgende Substitution

$$\begin{matrix} -\alpha, & -\beta, & -\gamma \\ -\alpha', & -\beta', & -\gamma' \\ -\alpha'', & -\beta'', & -\gamma'' \end{matrix}$$

in g übergeht; setzt man aber $-\alpha$ für α, $-\beta$ für β, u. s. w., in dem Werte von k, so entsteht $-k$, daher würde diese Substitution der Substitution S ungleichartig sein und daher jede ternäre Form, welche eine andere auf die eine Weise enthält, ebendieselbe auch auf die andere Weise enthalten. Eine derartige Unterscheidung wird daher hier ganz verbannt, da sie bei ternären Formen nichts nützt.

II. Bezeichnet man mit F, G die zu f, g adjungierten Formen, so werden die Coefficienten in F durch die Coefficienten in f bestimmt und die Coefficienten in G durch die Werte der Coefficienten der Form g, welche aus den Gleichungen, die die Substitution S liefert, bekannt sind. Drückt man die Coefficienten der Form f durch Buchstaben aus, so bestätigt man aus der Vergleichung der Werte der Coefficienten der Formen F, G ohne Mühe, dass F die Form G enthält und in sie durch die Substitution (S')

$$\begin{matrix} \beta'\gamma''-\beta''\gamma', & \gamma'\alpha''-\gamma''\alpha', & \alpha'\beta''-\alpha''\beta' \\ \beta''\gamma-\beta\gamma'', & \gamma''\alpha-\gamma\alpha'', & \alpha''\beta-\alpha\beta'' \\ \beta\gamma'-\beta'\gamma, & \gamma\alpha'-\gamma'\alpha, & \alpha\beta'-\alpha'\beta \end{matrix}$$

übergeht. Die Rechnung, welche keinen Schwierigkeiten unterliegt, schreiben wir nicht her.

III. Die Form g geht offenbar durch die Substitution (S'')

$$\begin{matrix} \beta'\gamma''-\beta''\gamma', & \beta''\gamma-\beta\gamma'', & \beta\gamma'-\beta'\gamma \\ \gamma'\alpha''-\gamma''\alpha', & \gamma''\alpha-\gamma\alpha'', & \gamma\alpha'-\gamma'\alpha \\ \alpha'\beta''-\alpha''\beta', & \alpha''\beta-\alpha\beta'', & \alpha\beta'-\alpha'\beta \end{matrix}$$

in dieselbe Form über, in welche die Form f durch die folgende Substitution

$$\begin{matrix} k, & 0, & 0 \\ 0, & k, & 0 \\ 0, & 0, & k \end{matrix}$$

übergeht, d. h. sie geht in diejenige Form über, welche entsteht, wenn man die einzelnen Coefficienten der Form f mit k^2 multipliciert. Diese Form bezeichnen wir mit f'.

IV. Ganz auf dieselbe Weise zeigt man, dass die Form G durch die Substitution (S''')

$$\begin{matrix} \alpha, & \alpha', & \alpha'' \\ \beta, & \beta', & \beta'' \\ \gamma, & \gamma', & \gamma'' \end{matrix}$$

übergeht in eine Form, die aus F entsteht, wenn man die einzelnen Coefficienten von F mit k^2 multipliciert. Diese Form werden wir mit F' bezeichnen.

Wir sagen, die Substitution S''' entstehe durch Transposition der Substitution S; dann wird offenbar S wiederum durch Transposition der Substitution S''' und von den Substitutionen S', S'' die eine durch Transposition der andern hervorgehen. — Die Substitution S' kann passend die Adjungierte der Substitution S genannt werden, daher auch S'' der Substitution S''' adjungiert ist.

269.

Wenn nicht nur die Form f die Form g, sondern auch diese jene Form enthält, so werden die Formen f, g **äquivalent** genannt. In diesem Falle geht daher nicht nur D in E, sondern auch E in D auf, woraus leicht folgt, dass $D = E$ sein muss. Umgekehrt aber sind, wenn die Form f die Form g mit derselben Determinante enthält, diese beiden Formen äquivalent. Denn es ist (wenn man dieselben Bezeichnungen anwendet wie im vorigen Artikel und den Fall, wo $D = 0$ ist, ausnimmt) $k = \pm 1$, und daher die Form f', in welche g durch die Substitution S'' übergeht, mit f identisch oder f unter g enthalten. Ferner ist klar, dass in diesem Falle auch die zu f, g adjungierten Formen F, G unter einander äquivalent sind und die letztere in die erstere durch die Substitution S''' übergeht. Schliesslich werden umgekehrt, wenn die Formen F, G als äquivalent vorausgesetzt werden und die erstere in die letztere übergeht durch die Substitution T, auch die Formen f, g äquivalent sein und es wird f in g durch die zu T adjungierte Substitution und g in f durch diejenige Substitution, welche durch Transposition von T entsteht, übergehen. Denn durch diese beiden Substitutionen respective geht die zu F adjungierte Form in die zu G adjungierte und diese in jene über; diese beiden Formen entstehen aber aus f, g durch Multiplikation der einzelnen Coefficienten mit D, woraus ohne Schwierigkeit folgt, dass durch eben dieselben Substitutionen f in g und g in f respective übergeht.

270.

Wenn die ternäre Form f die ternäre Form f' und diese wiederum die Form f'' enthält, so wird auch f die Form f'' enthalten. Denn man sieht leicht, dass, wenn

f in f' durch die Substitution	f' in f'' durch die Substitution
$\alpha,\ \beta,\ \gamma$	$\delta,\ \varepsilon,\ \zeta$
$\alpha',\ \beta',\ \gamma'$	$\delta',\ \varepsilon',\ \zeta'$
$\alpha'',\ \beta'',\ \gamma''$	$\delta'',\ \varepsilon'',\ \zeta''$

übergeht, f in f'' transformiert wird durch die Substitution:

$$\begin{matrix} \alpha\delta + \beta\delta' + \gamma\delta'', & \alpha\varepsilon + \beta\varepsilon' + \gamma\varepsilon'', & \alpha\zeta + \beta\zeta' + \gamma\zeta'' \\ \alpha'\delta + \beta'\delta' + \gamma'\delta'', & \alpha'\varepsilon + \beta'\varepsilon' + \gamma'\varepsilon'', & \alpha'\zeta + \beta'\zeta' + \gamma'\zeta'' \\ \alpha''\delta + \beta''\delta' + \gamma''\delta'', & \alpha''\varepsilon + \beta''\varepsilon' + \gamma''\varepsilon'', & \alpha''\zeta + \beta''\zeta' + \gamma''\zeta''. \end{matrix}$$

In dem Falle also, wo f der Form f' und f' der Form f'' äquivalent ist, wird auch die Form f der Form f'' äquivalent sein. — Übrigens ist ohne Weiteres klar, wie diese Sätze auf mehrere Formen anzuwenden sind.

271.

Hieraus geht bereits hervor, dass alle ternären Formen, ebenso wie die binären, in Klassen eingeteilt werden können, indem man äquivalente Formen zu derselben Klasse, nichtäquivalente Formen zu verschiedenen Klassen rechnet. Formen mit verschiedenen Determinanten werden daher sicher zu verschiedenen Klassen gehören, und somit wird es unendlich viele Klassen von ternären Formen geben; die zu derselben Determinante gehörigen ternären Formen aber bilden bald eine grössere, bald eine kleinere Anzahl von Klassen; was jedoch als Haupteigenschaft dieser Formen zu betrachten ist, ist das, **dass sämtliche Formen mit derselben gegebenen Determinante stets eine endliche Anzahl von Klassen bilden.** Der ausführlicheren Entwicklung dieses sehr wichtigen Satzes müssen wir die Darlegung des folgenden wesentlichen Unterschiedes, welcher unter den ternären Formen stattfindet, vorausschicken.

Gewisse ternäre Formen sind so beschaffen, dass durch sie ohne Unterschied positive und negative Zahlen dargestellt werden können, z. B. die Form $x^2 + y^2 - z^2$, weshalb sie **indefinite Formen** genannt werden. Dagegen lassen sich durch andere negative Zahlen nicht darstellen, sondern nur positive (ausser der Null, welche entsteht, wenn man die einzelnen Unbestimmten gleich 0 setzt), z. B. $x^2 + y^2 + z^2$, weshalb sie **positive Formen** genannt werden; endlich können durch andere wieder keine positiven Zahlen dargestellt werden, wie z. B. durch $-x^2 - y^2 - z^2$, weshalb dieselben **negative Formen** heissen. Die positiven und negativen Formen werden mit gemeinschaftlichem Namen **definite Formen** genannt. Im Folgenden geben wir bereits einige Kriterien, vermittelst deren diese Beschaffenheit der Formen erkannt werden kann.

Multipliciert man die ternäre Form

$$f = ax^2 + a'x'^2 + a''x''^2 + 2bx'x'' + 2b'xx'' + 2b''xx'$$

der Determinante D mit a und bezeichnet man die Coëfficienten der zu f adjungierten Form ebenso wie im Artikel 267 mit A, A', A'', B, B', B'', so ergiebt sich:

$$(ax + b''x' + b'x'')^2 - A''x'^2 + 2Bx'x'' - A'x''^2 = g;$$

multipliciert man nochmals mit A', so folgt:

$$A'(ax + b''x' + b'x'')^2 - (A'x'' - Bx')^2 + aDx'^2 = h.$$

Hieraus geht sogleich hervor, dass, wenn sowohl A' als aD negative Zahlen sind, sämtliche Werte von h negativ sind, weshalb offenbar durch die Form f nur solche Zahlen dargestellt werden können, deren Vorzeichen dem Vorzeichen von aA' entgegengesetzt, d. h. identisch mit dem Vorzeichen von a, oder entgegengesetzt dem Vorzeichen von D ist. In diesem Falle ist also f eine definite Form und zwar eine positive oder negative, je nachdem a positiv oder negativ, oder je nachdem D negativ oder positiv ist.

Sind aber entweder beide Zahlen aD, A' positiv oder die eine positiv, die andere negativ (keine gleich 0), so sieht man leicht, dass h durch gehörige Bestimmung der Grössen x, x', x'' sowohl positive als auch negative Werte erhalten kann. Daher wird in diesem Falle f Werte erhalten können, die mit demselben Vorzeichen oder mit entgegengesetztem Vorzeichen wie aA' behaftet sind, und daher wird f eine indefinite Form sein.

In dem Falle, wo $A' = 0$, aber nicht $a = 0$ ist, folgt:

$$g = (ax + b''x' + b'x'')^2 - x'(A''x' - 2Bx'').$$

Giebt man x' einen willkürlichen Wert (der jedoch nicht gleich 0) und nimmt man x'' so an, dass $\frac{A''x'}{2B} - x''$ dasselbe Vorzeichen erhält wie Bx' (dass dies möglich ist, sieht man leicht, da B nicht gleich Null sein kann; denn sonst würde $B^2 - A'A'' = aD = 0$ und daher $D = 0$ sein, welchen Fall wir ausgeschlossen haben), so wird $x'(A''x' - 2Bx'')$ eine positive Grösse, woraus leicht hervorgeht, dass x derart bestimmt werden kann, dass g einen negativen Wert erhält. Offenbar können diese Werte auch so angenommen werden, dass sie, wenn es gewünscht wird, sämtlich ganze Zahlen werden. Endlich ist klar, dass, wenn x', x'' beliebige Werte beigelegt werden, x so gross angenommen werden kann, dass g positiv wird. In diesem Falle ist daher f eine indefinite Form.

Ist endlich $a = 0$, so wird

$$f = a'x'^2 + 2bx'x'' + a''x''^2 + 2x(b''x' + b'x'').$$

Nimmt man daher x', x'' nach Belieben, jedoch so an, dass $b''x' + b'x''$ nicht gleich 0 ist (was offenbar möglich ist, wofern nicht gleichzeitig b' und b'' gleich 0 sind; dann würde aber $D = 0$ sein), so sieht man leicht, dass x so bestimmt werden kann, dass f sowohl positive als auch negative Werte erhält. Daher ist auch in diesem Falle f eine indefinite Form.

Auf dieselbe Weise, wie wir hier aus den Zahlen aD, A' die Natur der Form f beurteilt haben, können auch aD und A'' angewendet werden, so dass f eine definite Form ist, wenn sowohl aD als auch A'' negativ ist, eine indefinite aber in allen übrigen Fällen. Und auf ganz dieselbe Weise kann demselben Zwecke auch die Betrachtung der Zahlen $a'D$ und A, oder der Zahlen $a'D$ und A'', oder der Zahlen $a''D$ und A oder endlich der Zahlen $a''D$ und A' dienen.

Aus allem diesen folgt, dass in einer definiten Form die sechs Zahlen A, A', A'', aD, $a'D$, $a''D$ negativ sind, und zwar sind in der positiven Form a, a', a'' positiv, D negativ, in der negativen aber a, a', a'' negativ und D positiv. Hieraus geht hervor, dass alle ternären Formen mit gegebener positiver Determinante in negative und indefinite Formen zerfallen, alle ternären Formen mit gegebener negativer Determinante in positive und indefinite, endlich dass es positive Formen mit positiver Determinante oder negative mit negativer Determinante überhaupt nicht giebt. — Ebendaraus ist leicht ersichtlich, dass einer definiten Form immer eine definite und zwar negative Form, einer indefiniten eine indefinite adjungiert ist.

Da sämtliche durch eine gegebene ternäre Form darstellbaren Zahlen offenbar auch durch alle dieser äquivalente Formen dargestellt werden können, so werden die in derselben Klasse enthaltenen ternären Formen entweder sämtlich indefinit oder sämtlich positiv oder sämtlich negativ sein. Daher wird man diese Benennungen der Formen auch auf die ganzen Klassen übertragen können.

272.

Den im vorigen Artikel aufgestellten Satz, dass sämtliche ternären Formen mit gegebener Determinante in eine endliche Anzahl von Klassen zerfallen, werden wir nach einer Methode beweisen, die derjenigen ähnlich ist, deren wir uns bei den binären Formen bedient haben, indem wir nämlich zeigen, erstens, auf welche Weise jede ternäre Form auf eine einfachere Form zurückgeführt werden kann, zweitens, dass die Anzahl der einfachsten Formen (zu denen man durch solche Reductionen gelangt) für jede gegebene Determinante endlich ist. Nehmen wir allgemein an, dass die ternäre Form $f = \begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$ mit der (von Null verschiedenen) Determinante D gegeben ist, welche durch die Substitution

$$(S) \qquad \begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{matrix}$$

in die äquivalente Form $g = \begin{pmatrix} m, & m', & m'' \\ n, & n', & n'' \end{pmatrix}$ übergeht, so dreht sich unsere Aufgabe darum, α, β, γ, ... so zu bestimmen, dass die Form g einfacher wird als f. Sind die den Formen f, g adjungierten Formen resp. $\begin{pmatrix} A, & A', & A'' \\ B, & B', & B'' \end{pmatrix}$, $\begin{pmatrix} M, & M', & M'' \\ N, & N', & N'' \end{pmatrix}$, welche mit F, G bezeichnet werden mögen, so geht nach Artikel 269 F in G durch die zu S abjungierte Substitution, G aber in F durch die aus der Transposition von S entstehende Substitution über. Die Zahl

$$\alpha\beta'\gamma'' + \alpha'\beta''\gamma + \alpha''\beta\gamma' - \alpha''\beta'\gamma - \alpha\beta''\gamma' - \alpha'\beta\gamma'',$$

welche entweder gleich $+1$ oder gleich -1 sein muss, bezeichnen wir mit k. Hiernach bemerken wir:

I. Ist $\gamma = 0$, $\gamma' = 0$, $\alpha'' = 0$, $\beta'' = 0$, $\gamma'' = 1$, so wird:

$$m = a\alpha^2 + 2b''\alpha\alpha' + a'\alpha'^2, \quad m' = a\beta^2 + 2b''\beta\beta' + a'\beta'^2, \quad m'' = a''$$
$$n = b\beta' + b'\beta, \quad n' = b\alpha' + b'\alpha, \quad n'' = a\alpha\beta + b''(\alpha\beta' + \beta\alpha') + a'\alpha'\beta'.$$

Ausserdem muss $\alpha\beta' - \beta\alpha'$ entweder gleich $+1$ oder gleich -1 sein. Hieraus geht hervor, dass die binäre Form (a, b'', a'), deren Determinante A'' ist, durch die Substitution $\alpha, \beta, \alpha', \beta'$ in die binäre Form (m, n'', m') mit der Determinante M'' verwandelt wird und daher wegen $\alpha\beta' - \beta\alpha' = \pm 1$ ihr äquivalent ist, weshalb $M'' = A''$ ist, was auch direct leicht bestätigt werden kann. Wenn daher nicht schon (a, b'', a') die einfachste Form in ihrer Klasse ist, so wird man $\alpha, \beta, \alpha', \beta'$ so bestimmen können, dass (m, n'', m') eine einfachere Form ist, und zwar folgt aus der Theorie der Äquivalenz der binären Formen leicht, dass dies so geschehen kann, dass m nicht grösser als $\sqrt{-\frac{4}{3}A''}$, falls A'' negativ ist, oder nicht grösser als $\sqrt{A''}$, falls A'' positiv ist, oder $m = 0$ ist, falls $A'' = 0$ ist, so dass in allen Fällen der (absolute) Wert von m sicher entweder Null ist oder wenigstens bis auf $\sqrt{\pm\frac{4}{3}A''}$ herabgedrückt werden kann. Auf diese Weise wird also die Form f auf eine andere zurückgeführt, die, wenn dies überhaupt möglich ist, einen kleineren ersten Coefficienten hat, und deren adjungierte Form denselben dritten Coefficienten hat, wie die zu f adjungierte Form F. Hierin besteht die **erste Reduction.**

II. Ist dagegen $\alpha = 1$, $\beta = 0$, $\gamma = 0$, $\alpha' = 0$, $\alpha'' = 0$, so ist $k = \beta'\gamma'' - \beta''\gamma' = \pm 1$; die zu S adjungierte Substitution ist daher:

$$\begin{matrix} \pm 1, & 0, & 0 \\ 0, & \gamma'', & -\beta'' \\ 0, & -\gamma', & \beta', \end{matrix}$$

und durch diese geht F in G über. Man hat daher:

$$\begin{aligned}
m &= a, \quad n' = b'\gamma'' + b''\gamma', \quad n'' = b'\beta'' + b''\beta' \\
m' &= a'\beta'^2 + 2b\beta'\beta'' + a''\beta''^2 \\
m'' &= a'\gamma'^2 + 2b\gamma'\gamma'' + a''\gamma''^2 \\
n &= a'\beta'\gamma' + b(\beta'\gamma'' + \gamma'\beta'') + a''\beta''\gamma'' \\
M' &= A'\gamma''^2 - 2B\gamma'\gamma'' + A''\gamma'^2 \\
N &= -A'\beta''\gamma'' + B(\beta'\gamma'' + \gamma'\beta'') - A''\beta'\gamma' \\
M'' &= A'\beta''^2 - 2B\beta'\beta'' + A''\beta'^2.
\end{aligned}$$

Hieraus geht hervor, dass die binäre Form (A'', B, A'), deren Determinante Da ist, durch die Substitution $\beta', -\gamma', -\beta'', \gamma''$ in die Form (M'', N, M') mit der Determinante Dm übergeht und daher (wegen $\beta'\gamma'' - \gamma'\beta'' = \pm 1$ oder

wegen $Da = Dm$) ihr äquivalent ist. Wenn daher nicht schon (A'', B, A') die einfachste Form ihrer Klasse ist, so können die Coefficienten $\beta', \gamma', \beta'', \gamma''$ derart bestimmt werden, dass (M'', N, M') eine einfachere Form ist, und zwar kann dies immer so geschehen, dass M'' abgesehen vom Vorzeichen nicht grösser ist als $\sqrt{\pm \frac{4}{3} Da}$. Auf diese Weise wird also die Form f auf eine andere mit demselben ersten Coefficienten zurückgeführt, deren adjungierte Form aber einen dritten Coefficienten hat, der, wenn dies überhaupt möglich ist, kleiner ist als der dritte Coefficient der zu f adjungierten Form F. Hierin besteht die **zweite Reduction.**

III. Wenn daher f eine ternäre Form ist, auf welche weder die erste noch die zweite Reduction anwendbar ist, d. h. welche durch keine der beiden Reductionen auf eine einfachere Form gebracht werden kann, so wird, abgesehen vom Vorzeichen, notwendig sowohl $a^2 \leqq \frac{4}{3} A''$, als auch $A''^2 \leqq \frac{4}{3} aD$ sein. Hieraus folgt: $a^4 \leqq \frac{16}{9} A''^2$ und daher $a^4 \leqq \frac{64}{27} aD$ oder $a^3 \leqq \frac{64}{27} D$ und $a \leqq \frac{4}{3} \sqrt[3]{D}$; hieraus wiederum $A''^2 \leqq \frac{16}{9} \sqrt[3]{D^4}$ und $A'' \leqq \frac{4}{3} \sqrt[3]{D^2}$. Solange demnach a oder A'' diese Grenzen noch überschreiten, wird notwendig eine oder die andere der vorstehenden Reductionen auf die Form f angewendet werden können. — Übrigens darf dieser Schluss nicht umgekehrt werden, da es jedenfalls öfter eintrifft, dass eine ternäre Form, bei welcher der erste Coefficient und der dritte Coefficient der adjungierten Form bereits unterhalb jener Grenzen liegen, trotzdem durch die eine oder andere Reduction noch einfacher gemacht werden kann.

IV. Wenn nun aber auf eine beliebige gegebene ternäre Form mit der Determinante D abwechselnd die erste und zweite Reduction angewandt werden, d. h. wenn auf sie selbst die erste, auf die dadurch entstehende Form die zweite oder erste, auf die so sich ergebende Form wiederum die erste oder zweite Reduction, u. s. w., angewandt wird, so ist klar, dass man schliesslich notwendig zu einer Form gelangen wird, auf welche keine der beiden Reductionen mehr angewandt werden kann. Denn da die absolute Grösse sowohl der ersten Coefficienten der auf diese Weise sich ergebenden Formen, als auch der dritten Coefffcienten der zu ihnen adjungierten Formen beständig in abwechselnder Weise dieselbe bleibt oder abnimmt, so wird dieses Verfahren notwendig irgendwo ein Ende haben, da sonst zwei unendliche Reihen beständig abnehmender Zahlen erhalten würden. Hieraus haben wir bereits den schönen **Satz** erhalten: Jede ternäre Form mit der Determinante D lässt sich auf eine andere äquivalente Form bringen, bei welcher der erste Coefficient nicht grösser als $\frac{4}{3}\sqrt[3]{D}$ und der dritte Coefficient der zu ihr adjungierten Form nicht grösser als $\frac{4}{3}\sqrt[3]{D^2}$, abgesehen vom Vorzeichen, ist, falls nämlich die gegebene Form diese Eigenschaften noch nicht besitzt. — Übrigens

hätten wir an Stelle des ersten Coefficienten der Form f und des dritten Coefficienten der zu ihr adjungierten Form in ganz analoger Weise auch entweder den ersten Coefficienten der Form selbst und den zweiten der adjungierten, oder den zweiten der Form selbst und den ersten oder dritten der adjungierten oder den dritten der Form selbst und den ersten oder zweiten der adjungierten behandeln können und würden auf diesen Wegen ebenso zu dem von uns beabsichtigten Ziele gelangt sein; es ist jedoch zweckmässig, beständig an einer Methode festzuhalten, um die hierher gehörigen Operationen um so leichter auf einen bestimmten Algorithmus reducieren zu können. Schliesslich bemerken wir, dass für die beiden Coefficienten, von denen wir gezeigt haben, wie sie sich unter bestimmte Grenzen herabdrücken lassen, noch kleinere Grenzen festgestellt werden können, wenn man die definiten Formen von den indefiniten trennt; doch ist dies für unsern gegenwärtigen Zweck nicht erforderlich.

273.

Wir geben im Folgenden einige Beispiele, durch welche die vorstehend angegebenen Regeln deutlicher werden.

Beispiel 1. Ist $f=\begin{pmatrix}19, & 21, & 50\\ 15, & 28, & 1\end{pmatrix}$, so ist $F=\begin{pmatrix}-825, & -166, & -398\\ 257, & 573, & -370\end{pmatrix}$ und $D=-1$. Da (19, 1, 21) eine reducierte binäre Form ist, der eine andere mit kleinerem ersten Gliede als 19 nicht äquivalent ist, so ist hier die erste Reduction nicht anwendbar; dagegen findet man, dass die binäre Form $(A'', B, A') = (-398, 257, -166)$ nach der Theorie der Äquivalenz der binären Formen in eine einfachere äquivalente $(-2, 1, -10)$ transformierbar ist, und zwar geht sie in dieselbe über durch die Substitution 2, 7, 3, 11. Setzt man daher $\beta'=2$, $\gamma'=-7$, $\beta''=-3$, $\gamma''=11$, so ist auf die Form f die Substitution $\begin{Bmatrix}1, & 0, & 0\\ 0, & 2, & -7\\ 0, & -3, & 11\end{Bmatrix}$ anzuwenden, und durch diese geht sie über in die Form $\begin{pmatrix}19, & 354, & 4769\\ -1299, & 301, & -82\end{pmatrix}=f'$. Der dritte Coefficient der zu dieser adjungierten Form ist -2, in welcher Hinsicht f' für einfacher zu halten ist als f.

Auf die Form f' lässt sich die erste Reduction anwenden. Da nämlich die binäre Form $(19, -82, 354)$ in die Form $(1, 0, 2)$ durch die Substitution 13, 4, 3, 1 übergeht, so ist auf die Form f' die Substitution $\begin{Bmatrix}13, & 4, & 0\\ 3, & 1, & 0\\ 0, & 0, & 1\end{Bmatrix}$ anzuwenden, durch welche sie übergeht in $\begin{pmatrix}1, & 2, & 4769\\ -95, & 16, & 0\end{pmatrix}=f''$.

Auf die Form f'', welcher die Form $\begin{pmatrix}-513, & -4513, & -2\\ -95, & 32, & 1520\end{pmatrix}$ adjungiert ist, lässt sich von Neuem die zweite Reduction anwenden. Es geht nämlich

die Form $(-2, -95, -4513)$ durch die Substitution $47, 1, -1, 0$ über in $(-1, 1, -2)$; daher ist auf f'' die Substitution $\begin{Bmatrix}1, & 0, & 0\\ 0, & 47, & -1\\ 0, & 1, & 0\end{Bmatrix}$ anzuwenden, wodurch sie übergeht in $\begin{pmatrix}1, & 257, & 2\\ 1, & 0, & 16\end{pmatrix} = f'''$. Der erste Coefficient dieser lässt sich durch die erste Substitution nicht weiter erniedrigen, ebensowenig der dritte Coefficient der zu ihr adjungierten Form durch die zweite.

Beispiel 2. Ist die Form $\begin{pmatrix}10, & 26, & 2\\ 7, & 0, & 4\end{pmatrix} = f$, welcher die Form $\begin{pmatrix}-3, & -20, & -244\\ 70, & -28, & 8\end{pmatrix}$ adjungiert und deren Determinante gleich 2 ist, gegeben, so findet man, indem man abwechselnd die zweite und erste Reduction anwendet, der Reihe nach

die Substitutionen	durch welche übergeht	in
$\begin{Bmatrix}1, & 0, & 0\\ 0, & -1, & 0\\ 0, & 4, & -1\end{Bmatrix}$	f	$\begin{pmatrix}10, & 2, & 2\\ -1, & 0, & -4\end{pmatrix} = f'$
$\begin{Bmatrix}0, & -1, & 0\\ 1, & -2, & 0\\ 0, & 0, & 1\end{Bmatrix}$	f'	$\begin{pmatrix}2, & 2, & 2\\ 2, & -1, & 0\end{pmatrix} = f''$
$\begin{Bmatrix}1, & 0, & 0\\ 0, & -1, & 0\\ 0, & 2, & -1\end{Bmatrix}$	f''	$\begin{pmatrix}2, & 2, & 2\\ -2, & 1, & -2\end{pmatrix} = f'''$
$\begin{Bmatrix}1, & 0, & 0\\ 1, & 1, & 0\\ 0, & 0, & 1\end{Bmatrix}$	f'''	$\begin{pmatrix}0, & 2, & 2\\ -2, & -1, & 0\end{pmatrix} = f''''$

Die Form f'''' kann weder durch die erste noch durch die zweite Reduction weiter herabgedrückt werden.

274.

Hat man eine ternäre Form, bei welcher der erste Coefficient sowie der dritte Coefficient der zu ihr adjungierten Form nach den vorstehend angegebenen Methoden soweit als möglich erniedrigt sind, so liefert die folgende Methode eine weitere Reduction.

Behält man dieselben Bezeichnungen bei wie im Artikel 272 und setzt $\alpha = 1, \alpha' = 0, \beta' = 1, \alpha'' = 0, \beta'' = 0, \gamma'' = 1$, d. h. wendet man die Substitution

$$\begin{matrix}1, \beta, \gamma,\\ 0, 1, \gamma'\\ 0, 0, 1\end{matrix}$$

an, so wird:

$$m = a,\ m' = a' + 2b''\beta + a\beta^2,\ m'' = a'' + 2b\gamma' + 2b'\gamma + a\gamma^2 + 2b''\gamma\gamma' + a'\gamma'^2$$
$$n = b + a'\gamma' + b'\beta + b''(\gamma + \beta\gamma') + a\beta\gamma,\ n' = b' + a\gamma + b''\gamma',\ n'' = b'' + a\beta;$$

ausserdem:

$$M'' = A'',\quad N = B - A''\gamma',\quad N' = B' - N\beta - A''\gamma.$$

Durch eine solche Substitution werden also die Coefficienten a, A'', welche durch die vorigen Reductionen erniedrigt worden sind, nicht verändert; daher besteht unsere Aufgabe darin, durch eine geeignete Bestimmung von β, γ, γ' Erniedrigungen in den andern Coefficienten zu erhalten. Zu diesem Zwecke bemerken wir zunächst, dass, wenn $A'' = 0$ ist, angenommen werden kann, dass auch $a = 0$ sei; denn wenn a nicht gleich 0 wäre, so würde die erste Reduction nochmals anwendbar sein, da einer jeden binären Form mit der Determinante 0 eine Form wie $(0, 0, h)$ oder eine Form, deren erster Coefficient gleich 0 ist, äquivalent ist (Vgl. Artikel 215). Aus ganz analogem Grunde darf man voraussetzen, dass, wenn $a = 0$ ist, auch $A'' = 0$ sei, so dass von den Zahlen a, A'' entweder keine gleich 0 ist oder beide gleich 0 sind.

Im ersteren Falle ist klar, dass β, γ, γ' so bestimmt werden können, dass ohne Rücksicht auf das Vorzeichen n'', N, N' bezüglich nicht grösser sind als $\frac{1}{2}a$, $\frac{1}{2}A''$, $\frac{1}{2}A''$. So wird in dem ersten Beispiel des vorigen Artikels die letzte Form $\begin{pmatrix}1, & 257, & 2\\ 1, & 0, & 16\end{pmatrix}$, welcher die Form $\begin{pmatrix}-513, & -2, & -1\\ 1, & -16, & 32\end{pmatrix}$ adjungiert ist, durch die Substitution $\begin{Bmatrix}1, & -16, & 16\\ 0, & 1, & -1\\ 0, & 0, & 1\end{Bmatrix}$ übergehen in die folgende: $\begin{pmatrix}1, & 1, & 1\\ 0, & 0, & 0\end{pmatrix} = f'''$, welcher die Form $\begin{pmatrix}-1, & -1, & -1\\ 0, & 0, & 0\end{pmatrix}$ adjungiert ist.

Im letzteren Falle, wo $a = A'' = 0$ und daher auch $b'' = 0$ ist, wird

$$m = 0,\quad m' = a',\quad m'' = a'' + 2b\gamma' + 2b'\gamma + a'\gamma'^2$$
$$n = b + a'\gamma' + b'\beta.\quad n' = b',\quad n'' = 0.$$

Es ist daher:

$$D = a'b'^2 = m'n'^2$$

und man sieht leicht, dass β und γ' so bestimmt werden können, dass n gleich dem absolut kleinsten Reste von b nach einem Modul wird, welcher der grösste gemeinschaftliche Teiler von a', b' ist, d. h. dass n nicht grösser wird als die Hälfte dieses Teilers ohne Rücksicht auf das Vorzeichen, und daher $n = 0$ ist, so oft a', b' prim zu einander sind. Sind β, γ' auf diese Weise bestimmt, so kann der Wert von γ so angenommen werden, dass m'' ohne Rücksicht auf das Vorzeichen nicht grösser ist als b'; dies würde allerdings unmöglich sein, wenn $b' = 0$ ist; dann würde aber $D = 0$ sein, welchen Fall wir ausgeschlossen haben. So wird für die letzte Form im zweiten Beispiel des vorigen Artikels $n = -2 - \beta + 2\gamma'$, woraus,

wenn $\beta = -2$, $\gamma' = 0$ gesetzt wird, $n = 0$ folgt, ferner $m'' = 2 - 2\gamma$ und, wenn man $\gamma = 1$ setzt, $m'' = 0$. Wir erhalten daher die Substitution $\begin{Bmatrix}1, & -2, & 1\\ 0, & 1, & 0\\ 0, & 0, & 1\end{Bmatrix}$, durch welche jene Form übergeht in $\begin{pmatrix}0, & 2, & 0\\ 0, & -1, & 0\end{pmatrix} = f'''''$.

275.

Hat man eine Reihe von äquivalenten ternären Formen $f, f', f'', f''', \ldots$ und die Transformationen einer jeden dieser Formen in die folgende, so leitet man aus der Transformation von f in f' und von f' in f'' nach Artikel 270 die Transformation der Form f in f'' her; aus dieser und der Transformation der Form f'' in f''' folgt die Transformation der Form f in f''' u. s. w., und offenbar kann auf diese Weise die Transformation der Form f in jede beliebige andere Form der Reihe gefunden werden. Und da aus der Transformation der Form f in irgend eine andere äquivalente Form g die Transformation der Form g in f (S'' aus S Artikel 268, 269) abgeleitet werden kann, so kann auf diese Weise die Transformation jeder beliebigen Form der Reihe $f', f'', \ldots$ in die erste f gefunden werden. — So findet man für die Formen des ersten Beispiels im vorigen Artikel die Substitutionen:

$$\begin{array}{rrr|rrr|rrr} 13, & 4, & 0 & 13, & 188, & -4 & 13, & -20, & 16\\ 6, & 2, & -7 & 6, & 87, & -2 & 6, & -9, & 7\\ -9, & -3, & 11 & -9, & -130, & 3 & -9, & 14, & -11, \end{array}$$

durch welche die Form f bezüglich in f'', f''', f'''' übergeht, und aus der letzten Substitution die folgende $\begin{Bmatrix}1, & 4, & 4\\ 3, & 1, & 5\\ 3, & -2, & 3\end{Bmatrix}$, durch welche f'''' in f übergeht. — Auf ähnliche Weise ergeben sich im zweiten Beispiel des vorigen Artikels die Substitutionen

$$\begin{array}{rrr|rrr} 1, & -1, & 1 & 2, & -3, & -1\\ -3, & 4, & -3 & 3, & 1, & 0\\ 10, & -14, & 11 & 2, & 4, & 1, \end{array}$$

durch welche respective die Form $\begin{pmatrix}10, & 26, & 2\\ 7, & 0, & 4\end{pmatrix}$ in $\begin{pmatrix}0, & 2, & 0\\ 0, & -1, & 0\end{pmatrix}$ und diese wieder in jene übergeht.

276.

Satz. Die Anzahl der Klassen, in welche sämtliche ternären Formen mit gegebener Determinante zerfallen, ist stets endlich.

Beweis. I. Die Anzahl sämtlicher Formen $\begin{pmatrix}a, & a', & a''\\ b, & b', & b''\end{pmatrix}$ mit der gegebenen Determinante D, in denen $a = 0$, $b'' = 0$, b nicht grösser als die Hälfte des

grössten gemeinschaftlichen Teilers von a', b' und a'' nicht grösser als b' ist, ist offenbar endlich. Denn da $a'b'^2 = D$ sein muss, so können für b' keine andern Werte genommen werden als $+1$, -1 und die Wurzeln aus den in D aufgehenden Quadraten (wenn es ausser 1 noch andere giebt) und zwar mit positivem oder negativem Vorzeichen versehen, und die Anzahl dieser Werte ist endlich. Für die einzelnen Werte von b' aber ist der Wert von a' bestimmt und die Werte von b, a'' sind offenbar auf eine endliche Anzahl beschränkt.

II. Ebenso ist die Anzahl aller Formen $\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$ mit der Determinante D, in welchen a nicht gleich 0 und nicht grösser als $\frac{4}{3}\sqrt[3]{\pm D}$, $b''^2 - aa' = A''$ nicht gleich Null und nicht grösser als $\frac{4}{3}\sqrt[3]{D^2}$, b'' nicht grösser als $\frac{1}{2}a$, $ab - b'b'' = B$ und $a'b' - bb'' = B'$ nicht grösser als $\frac{1}{2}A''$ sind, eine endliche. Denn die Anzahl aller Combinationen der Werte von a, b'', A'', B, B' ist endlich; sind diese aber einzeln bestimmt, so werden auch die übrigen Coefficienten a', b, b', a'' der Form und die Coefficienten

$$b^2 - a'a'' = A, \quad b'^2 - aa'' = A', \quad a''b'' - bb' = B''$$

der adjungierten Form bestimmt sein durch folgende Gleichungen:

$$a' = \frac{b''^2 - A''}{a}, \quad A' = \frac{B^2 - aD}{A''}, \quad A = \frac{B'^2 - a'D}{A''}, \quad B'' = \frac{BB' + b''D}{A''}$$

$$b = \frac{AB - B'B''}{D} = -\frac{Ba' + B'b''}{A''}, \quad b' = \frac{A'B' - BB''}{D} = -\frac{Bb'' + B'a}{A''}$$

$$a'' = \frac{b'^2 - A'}{a} = \frac{b^2 - A}{a'} = \frac{bb' + B''}{b''}.$$

Da nun alle jene Formen erhalten werden, wenn man aus allen Combinationen der Werte von a, b'', A'', B, B' diejenigen auswählt, für welche a', a'', b, b' ganze Werte erhalten, so ist die Anzahl jener offenbar endlich.

III. Sämtliche Formen in I und II bilden also zusammen eine endliche Anzahl von Klassen, die auch kleiner sein kann als die Anzahl der Formen, wenn irgend welche von diesen unter einander äquivalent sind. Da nun nach den vorhergehenden Untersuchungen jede ternäre Form mit der Determinante D notwendig irgend einer von jenen Formen äquivalent ist, d. h. zu irgend einer der Klassen, welche diese Formen bilden, gehört, so werden diese Klassen alle Formen mit der Determinante D umfassen, d. h. alle ternären Formen mit der Determinante D zerfallen in eine endliche Anzahl von Klassen.

277.

Die Regeln, nach denen alle Formen in I und II des vorigen Artikels ermittelt werden können, ergeben sich aus ihrer Entwicklung von selbst, weshalb es genügen wird, einige **Beispiele** anzuführen.

Für $D = 1$ ergeben sich folgende sechs (wegen der doppelten Vorzeichen) Formen I:

$$\begin{pmatrix} 0, & 1, 0 \\ 0, & \pm 1, 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & 1, \pm 1 \\ 0, & \pm 1, & 1 \end{pmatrix}.$$

In den Formen II können a und A'' keine andern Werte ausser $+1$ und -1 haben, und für die vier hieraus entspringenden Combinationen müssen b'', B und B' gleich 0 gesetzt werden; demnach entstehen die vier Formen:

$$\begin{pmatrix} 1, -1, 1 \\ 0, \quad 0, 0 \end{pmatrix}, \quad \begin{pmatrix} -1, 1, 1 \\ 0, 0, 0 \end{pmatrix}, \quad \begin{pmatrix} 1, 1, -1 \\ 0, 0, \quad 0 \end{pmatrix}, \quad \begin{pmatrix} -1, -1, -1 \\ 0, \quad 0, \quad 0 \end{pmatrix}.$$

Ebenso erhält man für $D = -1$ sechs Formen I und vier Formen II, nämlich:

$$\begin{pmatrix} 0, -1, 0 \\ 0, \pm 1, 0 \end{pmatrix}, \begin{pmatrix} 0, -1, \pm 1 \\ 0, \pm 1, \quad 0 \end{pmatrix}; \begin{pmatrix} 1, -1, -1 \\ 0, \quad 0, \quad 0 \end{pmatrix}, \begin{pmatrix} -1, 1, -1 \\ 0, 0, \quad 0 \end{pmatrix}, \begin{pmatrix} -1, -1, 1 \\ 0, \quad 0, 0 \end{pmatrix}, \begin{pmatrix} 1, 1, 1 \\ 0, 0, 0 \end{pmatrix}.$$

Für $D = 2$ ergeben sich sechs Formen I:

$$\begin{pmatrix} 0, & 2, 0 \\ 0, & \pm 1, 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & 2, \pm 1 \\ 0, & \pm 1, & 0 \end{pmatrix}$$

und acht Formen II:

$$\begin{pmatrix} 1, -1, 2 \\ 0, \quad 0, 0 \end{pmatrix}, \quad \begin{pmatrix} -1, 1, 2 \\ 0, 0, 0 \end{pmatrix}, \quad \begin{pmatrix} 1, 1, -2 \\ 0, 0, \quad 0 \end{pmatrix}, \quad \begin{pmatrix} -1, -1, -2 \\ 0, \quad 0, \quad 0 \end{pmatrix}$$

$$\begin{pmatrix} 1, -2, 1 \\ 0, \quad 0, 0 \end{pmatrix}, \quad \begin{pmatrix} -1, 2, 1 \\ 0, 0, 0 \end{pmatrix}, \quad \begin{pmatrix} 1, 2, -1 \\ 0, 0, \quad 0 \end{pmatrix}, \quad \begin{pmatrix} -1, -2, -1 \\ 0, \quad 0, \quad 0 \end{pmatrix}.$$

Übrigens ist die Anzahl der aus diesen Formen in diesen drei Fällen hervorgehenden Klassen viel kleiner als die Anzahl der Formen. Man bestätigt nämlich leicht, dass

I. Die Form $\begin{pmatrix} 0, 1, 0 \\ 0, 1, 0 \end{pmatrix}$ übergeht in

$$\begin{pmatrix} 0, & 1, 0 \\ 0, & -1, 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & 1, 1 \\ 0, & \pm 1, 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & 1, -1 \\ 0, & \pm 1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1, 1, -1 \\ 0, 0, \quad 0 \end{pmatrix}$$

respective durch die Substitutionen:

$$\begin{array}{ccc|ccc|ccc|ccc} 1, & 0, & 0 & 0, & 0, & 1 & 0, & 0, & 1 & 1, & 0, & -1 \\ 0, & 1, & 0 & 0, & 1, & -1 & 0, & 1, & 1 & 1, & 1, & -1 \\ 0, & 0, & -1 & \pm 1, & 1, & 0 & \pm 1, & -1, & -1 & 0, & -1, & 1, \end{array}$$

die Form $\begin{pmatrix} 1, 1, -1 \\ 0, 0, \quad 0 \end{pmatrix}$ aber in $\begin{pmatrix} 1, -1, 1 \\ 0, \quad 0, 0 \end{pmatrix}$, $\begin{pmatrix} -1, 1, 1 \\ 0, 0, 0 \end{pmatrix}$ durch blosse Vertauschung der Unbestimmten. Daher reducieren sich jene zehn ternären Formen mit der Determinante 1 auf die folgenden zwei: $\begin{pmatrix} 0, 1, 0 \\ 0, 1, 0 \end{pmatrix}$, $\begin{pmatrix} -1, -1, -1 \\ 0, \quad 0, \quad 0 \end{pmatrix}$; für die erstere kann man auch, wenn man lieber will, die

folgende nehmen: $\begin{pmatrix}1, 0, 0\\1, 0, 0\end{pmatrix}$. Da die erste Form indefinit, die zweite definit ist, so ist klar, dass jede indefinite ternäre Form mit der Determinante 1 der Form $x^2 + 2yz$, jede definite der Form $-x^2 - y^2 - z^2$ äquivalent ist.

II. Auf ganz analoge Weise findet man, dass jede indefinite ternäre Form mit der Determinante -1 der Form $-x^2 + 2yz$, jede definite der Form $x^2 + y^2 + z^2$ äquivalent ist.

III. Für die Determinante 2 können von den acht Formen II sogleich die zweite, sechste und siebente weggelassen werden, da sie aus der ersten durch blosse Permutation der Unbestimmten entstehen, und aus ähnlichem Grunde auch die fünfte, welche aus der dritten, und die achte, welche aus der vierten in gleicher Weise sich ergiebt. Die drei übrigen bilden mit den sechs Formen I drei Klassen; es geht nämlich $\begin{pmatrix}0, 2, 0\\0, 1, 0\end{pmatrix}$ in $\begin{pmatrix}0, & 2, 0\\0, & -1, 0\end{pmatrix}$ durch die Substitution $\begin{Bmatrix}1, & 0, & 0\\0, & 1, & 0\\0, & 0, & -1\end{Bmatrix}$ und die Form $\begin{pmatrix}1, & 1, & -2\\0, & 0, & 0\end{pmatrix}$ in

$$\begin{pmatrix}0, 2, 1\\0, 1, 0\end{pmatrix}, \quad \begin{pmatrix}0, & 2, 1\\0, & -1, 0\end{pmatrix}, \quad \begin{pmatrix}0, 2, & -1\\0, 1, & 0\end{pmatrix}, \quad \begin{pmatrix}0, & 2, & -1\\0, & -1, & 0\end{pmatrix}, \quad \begin{pmatrix}1, & -1, 2\\0, & 0, 0\end{pmatrix}$$

respective durch die Substitutionen über:

1, 0, 1	1, 0, −1	1, 0, 0	1, 0, 0	1, 0, 0
1, 2, 0	1, 2, 0	1, 2, −1	1, 2, 1	0, 1, 2
1, 1, 0	1, 1, 0	1, 1, −1	1, 1, 1	0, 1, 1.

Jede ternäre Form mit der Determinante 2 ist daher auf irgend eine von den folgenden drei Formen reducierbar:

$$\begin{pmatrix}0, 2, 0\\0, 1, 0\end{pmatrix}, \quad \begin{pmatrix}1, 1, -2\\0, 0, \;\; 0\end{pmatrix}, \quad \begin{pmatrix}-1, -1, -2\\0, \;\; 0, \;\; 0\end{pmatrix};$$

an Stelle der ersten kann man auch, wenn man lieber will, die Form $\begin{pmatrix}2, 0, 0\\1, 0, 0\end{pmatrix}$ nehmen. Offenbar aber wird jede definite ternäre Form notwendig der dritten $-x^2 - y^2 - 2z^2$ äquivalent sein, da die beiden ersten indefinit sind, jede indefinite aber der ersten oder zweiten und zwar der ersten $2x^2 + 2yz$, wenn ihr erster, zweiter und dritter Coefficient gleichzeitig gerade sind (da man leicht sieht, dass eine solche Form durch irgend eine Transformation in eine ähnliche Form übergeht und daher nicht der zweiten äquivalent sein kann), der zweiten $x^2 + y^2 - 2z^2$ aber, wenn ihr erster, zweiter und dritter Coefficient nicht gleichzeitig gerade sind, vielmehr einer, zwei oder alle drei ungerade sind (denn in eine solche Form lässt sich aus analogem Grunde die erste Form $2x^2 + 2yz$ durch keine Substitution transformieren).

Was somit in den Beispielen der Artikel 273, 274 sich ergiebt, dass nämlich die definite Form $\begin{pmatrix}19, 21, 50\\ 15, 28, 1\end{pmatrix}$ mit der Determinante -1 auf die Form $x^2+y^2+z^2$ und die indefinite Form $\begin{pmatrix}10, 26, 2\\ 7, 0, 4\end{pmatrix}$ mit der Determinante 2 auf die Form $2x^2-2yz$ oder (was auf dasselbe hinauskommt) auf die Form $2x^2+2yz$ zurückgeführt werden kann, hätte man nach den vorhergehenden Untersuchungen von vornherein sehen können.

278.

Durch eine ternäre Form, deren Unbestimmten x, x', x'' sind, werden einerseits Zahlen **dargestellt**, wenn man x, x', x'' bestimmte Werte beilegt, andrerseits binäre Formen durch Substitutionen von der Form:

$$x=mt+nu,\quad x'=m't+n'u,\quad x''=m''t+n''u,$$

wo $m, n, m', \ldots$ bestimmte Zahlen, t, u aber die Unbestimmten der dargestellten Form bezeichnen. Zu einer vollständigen Theorie der ternären Formen würde daher die Lösung folgender Aufgaben erforderlich sein:

I. Alle Darstellungen einer gegebenen Zahl durch eine gegebene ternäre Form zu finden.

II. Alle Darstellungen einer gegebenen binären Form durch eine gegebene ternäre Form zu finden.

III. Zu entscheiden, ob zwei gegebene ternäre Formen mit derselben gegebenen Determinante äquivalent sind oder nicht, und im ersteren Falle alle Transformationen der einen in die andere zu finden.

IV. Zu entscheiden, ob eine gegebene ternäre Form eine andere gegebene mit grösserer Determinante enthält oder nicht, und im ersteren Falle alle Transformationen der einen in die andere zu bestimmen.

Über diese Aufgaben, die bei weitem schwieriger sind, als die analogen bei den binären Formen, werden wir an anderer Stelle weitläufiger handeln; hier beschränken wir unsere Untersuchung darauf zu zeigen, wie die erste Aufgabe auf die zweite und die zweite auf die dritte sich reducieren lässt; die dritte werden wir aber für einige der einfachsten und die Theorie der binären Formen besonders beleuchtenden Fälle lösen lehren; die vierte werden wir hier ganz ausschliessen.

279.

Hülfssatz. Wenn drei beliebige ganze Zahlen a, a', a'' (welche jedoch nicht sämtlich zu gleicher Zeit Null sind) gegeben sind, so soll man sechs andere B, B', B'', C, C', C'' von solcher Beschaffenheit finden, dass

$$B'C''-B''C'=a,\quad B''C-BC''=a',\quad BC'-B'C=a''$$

wird.

Auflösung. Es sei α der grösste gemeinschaftliche Teiler von a, a', a'' und man nehme ganze Zahlen A, A', A'' so an, dass

$$Aa + A'a' + A''a'' = \alpha$$

wird. Ferner nehme man drei ganze Zahlen $\mathfrak{G}$, $\mathfrak{G}'$, $\mathfrak{G}''$ nach Belieben nur mit der Bedingung an, dass die drei Zahlen $\mathfrak{G}'A'' - \mathfrak{G}''A'$, $\mathfrak{G}''A - \mathfrak{G}A''$ $\mathfrak{G}A' - \mathfrak{G}'A$, die wir respective mit b, b', b'' und deren grössten gemeinschaftlichen Teiler wir mit β bezeichnen, nicht gleichzeitig gleich Null werden. Setzt man dann

$$a'b'' - a''b' = \alpha\beta C,\quad a''b - ab'' = \alpha\beta C',\quad ab' - a'b = \alpha\beta C'',$$

so sind offenbar C, C', C'' ganze Zahlen. Nimmt man schliesslich ganze Zahlen $\mathfrak{B}$, $\mathfrak{B}'$, $\mathfrak{B}''$ so an, dass

$$\mathfrak{B}b + \mathfrak{B}'b' + \mathfrak{B}''b'' = \beta$$

wird, setzt:

$$\mathfrak{B}a + \mathfrak{B}a' + \mathfrak{B}''a'' = h$$

und macht:

$$B = \alpha\mathfrak{B} - hA,\quad B' = \alpha\mathfrak{B}' - hA',\quad B'' = \alpha\mathfrak{B}'' - hA'',$$

so werden diese Werte von B, B', B'', C, C', C'' den vorgeschriebenen Bedingungen entsprechen.

Man findet nämlich:

$$aB + a'B' + a''B'' = 0$$

$$bA + b'A' + b''A'' = 0 \text{ und daher } bB + b'B' + b''B'' = \alpha\beta.$$

Nun wird aus den Werten von C', C'':

$$\begin{aligned}\alpha\beta\,(B'C'' - B''C') &= ab'B' - a'bB' - a''bB'' + ab''B'' \\ &= a\,(bB + b'B' + b''B'') - b\,(aB + a'B' + a''B'') = \alpha\beta a\end{aligned}$$

und daher $B'C'' - B''C' = a$ und auf ähnliche Weise findet man $B''C - BC'' = a'$, $BC' - B'C = a''$.

Im Übrigen muss die Analyse, durch welche diese Lösung gefunden worden ist, sowie die Methode, aus einer Lösung alle zu finden, hier weggelassen werden.

280.

Wir nehmen an, dass die binäre Form

$$at^2 + 2btu + cu^2 = \varphi,$$

deren Determinante gleich D sei, dargestellt werde durch die ternäre Form f, deren Unbestimmten x, x', x'' sind, wenn man setzt:

$$x = mt + nu,\quad x' = m't + n'u,\quad x'' = m''t + n''u,$$

und dass der Form f die Form F, deren Unbestimmten X, X', X'' sind, adjungiert sei. Dann bestätigt man leicht durch Rechnung (indem man die Coefficienten der Formen f, F mit besonderen Buchstaben bezeichnet)

oder leitet auch sogleich aus Artikel 268. II her, dass die Zahl D durch F dargestellt wird, wenn man setzt:

$$X = m'n'' - m''n',\quad X' = m''n - mn'',\quad X'' = mn' - m'n,$$

eine Darstellung der Zahl D, die passend der Darstellung der Form φ durch f adjungiert genannt werden kann. Wenn die Werte von X, X', X'' keinen gemeinschaftlichen Teiler haben, so werden wir diese Darstellung von D eine eigentliche, im andern Falle eine uneigentliche nennen und werden dieselben Benennungen auch der Darstellung der Form φ durch f, welcher jene Darstellung adjungiert ist, beilegen. Nun beruht die Auffindung aller eigentlichen Darstellungen der Zahl D durch die Form F auf folgenden Punkten:

I. Es giebt keine Darstellung von D durch F, welche nicht aus irgend einer Darstellung irgend einer Form mit der Determinante D durch die Form f abgeleitet werden könnte, d. h. einer solchen Darstellung adjungiert wäre.

Es sei nämlich irgend eine Darstellung von D durch F die folgende: $X = L$, $X' = L'$, $X'' = L''$; man nehme nach dem Hülfssatz des vorigen Artikels m, m', m'', n, n', n'' so an, dass

$$m'n'' - m''n' = L,\quad m''n - mn'' = L',\quad mn' - m'n = L''$$

wird, und es gehe f durch die Substitution

$$x = mt + nu,\quad x' = m't + n'u,\quad x'' = m''t + n''u$$

in die binäre Form $\varphi = at^2 + 2btu + cu^2$ über. Dann sieht man leicht, dass D die Determinante der Form φ und die gegebene Darstellung von D durch F der Darstellung jener durch f adjungiert ist.

Beispiel. Es sei $f = x^2 + x'^2 + x''^2$, und daher $F = -X^2 - X'^2 - X''^2$, $D = -209$ und eine Darstellung dieser durch F die folgende: $X = 1$, $X' = 8$, $X'' = 12$. Hieraus findet man für m, m', m'', n, n', n'' respective die folgenden Werte: $-20, 1, 1, -12, 0, 1$ und $\varphi = 402\,t^2 + 482\,tu + 145\,u^2$.

II. Wenn φ, χ eigentlich äquivalente binäre Formen sind, so wird jede Darstellung von D durch F, welche irgend einer Darstellung der Form φ durch f adjungiert ist, auch irgend einer Darstellung der Form χ durch f adjungiert sein.

Sind p, q die Unbestimmten der Form χ, geht ferner φ in χ über durch die eigentliche Substitution $t = \alpha p + \beta q$, $u = \gamma p + \delta q$ und ist irgend eine Darstellung der Form φ durch f die folgende:

$$(R)\qquad x = mt + nu,\quad x' = m't + n'u,\quad x'' = m''t + n''u,$$

so sieht man ohne Mühe, dass, wenn man

$$\begin{array}{lll} \alpha m + \gamma n = g, & \alpha m' + \gamma n' = g', & \alpha m'' + \gamma n'' = g'' \\ \beta m + \delta n = h, & \beta m' + \delta n' = h', & \beta m'' + \delta n'' = h'' \end{array}$$

setzt, die Form χ durch f dargestellt werden wird, wenn man

$$(R') \qquad x = gp + hq, \quad x' = g'p + h'q, \quad x'' = g''p + h''q$$

setzt, und führt man die Rechnung aus, so findet man (wegen $\alpha\delta - \beta\gamma = 1$):

$$g'h'' - g''h' = m'n'' - m''n', \quad g''h - gh'' = m''n - mn'', \quad gh' - g'h = mn' - m'n,$$

d. h. den Darstellungen R, R' ist dieselbe Darstellung von D durch F äquivalent.

So findet man, dass im vorigen Beispiele der Form φ die Form $\chi = 13p^2 - 10pq + 18q^2$ äquivalent ist, und zwar geht jene in diese über durch die eigentliche Substitution $t = -3p + q$, $u = 5p - 2q$. Hieraus findet man folgende Darstellung der Form χ durch f: $x = 4q$, $x' = -3p + q$, $x'' = 2p - q$, aus der sich dieselbe Darstellung der Zahl -209 ergiebt, von welcher wir ausgegangen waren.

III. Wenn endlich zwei binäre Formen φ, χ mit der Determinante D, deren Unbestimmten t, u; p, q sind, durch f dargestellt werden können und irgend einer Darstellung der einen dieselbe eigentliche Darstellung von D durch F adjungiert ist, wie irgend einer Darstellung der andern, so sind jene Formen notwendig eigentlich äquivalent. Wir nehmen an, dass φ durch f dargestellt werde, wenn man setzt:

$$x = mt + nu, \quad x' = m't + n'u, \quad x'' = m''t + n''u,$$

χ aber, wenn man setzt:

$$x = gp + hq, \quad x' = g'p + h'q, \quad x'' = g''p + h''q,$$

und dass

$$\begin{aligned} m'n'' - m''n' &= g'h'' - g''h' = L \\ m''n - mn'' &= g''h - gh'' = L' \\ mn' - m'n &= gh' - g'h = L'' \end{aligned}$$

sei. Man nehme ganze Zahlen l, l', l'' so an, dass $Ll + L'l' + L''l'' = 1$ wird, und man setze:

$$\begin{aligned} n'l'' - n''l' &= M, \quad n''l - nl'' = M', \quad nl' - n'l = M'' \\ l'm'' - l''m' &= N, \quad l''m - lm'' = N', \quad lm' - l'm = N''. \end{aligned}$$

Endlich setze man:

$$\begin{aligned} gM + g'M' + g''M'' &= \alpha, \quad hM + h'M' + h''M'' = \beta \\ gN + g'N' + g''N'' &= \gamma, \quad hN + h'N' + h''N'' = \delta. \end{aligned}$$

Hieraus ergiebt sich leicht:

$$\begin{aligned} \alpha m + \gamma n &= g - l(gL + g'L' + g''L'') = g \\ \beta m + \delta n &= h - l(hL + h'L' + h''L'') = h \end{aligned}$$

und ebenso:

$$\alpha m' + \gamma n' = g', \quad \beta m' + \delta n' = h', \quad \alpha m'' + \gamma n'' = g'', \quad \beta m'' + \delta n'' = h''.$$

Hieraus geht hervor, dass $mt+nu$, $m't+n'u$, $m''t+n''u$ durch die Substitution

$$(S)\qquad t=\alpha p+\beta q,\quad u=\gamma p+\delta q$$

übergeht in: $gp+hq$, $g'p+h'q$, $g''p+h''q$ respective, woraus erhellt, dass φ durch die Substitution S in dieselbe Form übergeht, in welche f übergeht, wenn man setzt:

$$x=gp+hq,\quad x'=g'p+h'q,\quad x''=g''p+h''q,$$

und somit in die Form χ, der sie mithin äquivalent ist. Schliesslich findet man nach den gehörigen Reductionen leicht:

$$\alpha\delta-\beta\gamma=(Ll+L'l'+L''l'')^2=1,$$

weshalb die Substitution S eine eigentliche ist und die Formen φ, χ eigentlich äquivalent sind.

Aus diesen Bemerkungen ergeben sich folgende Regeln zur Auffindung sämtlicher eigentlichen Darstellungen von D durch F: Man entwickle sämtliche Klassen der binären Formen mit der Determinante D und wähle aus jeder einzelnen eine Form nach Belieben aus; man suche alle eigentlichen Darstellungen dieser einzelnen Formen durch f (indem man diejenigen weglässt, die etwa nicht durch f dargestellt werden können) und aus diesen einzelnen Darstellungen leite man die Darstellungen von D durch F her. Aus I und II geht hervor, dass auf diese Weise alle möglichen eigentlichen Darstellungen erhalten werden und somit die Lösung vollständig ist; aus III folgt, dass die Transformationen der Formen aus verschiedenen Klassen sicher verschiedene Darstellungen hervorbringen.

281.

Die Ermittlung der uneigentlichen Darstellungen einer gegebenen Zahl D durch die Form F lässt sich leicht auf den vorigen Fall zurückführen. Es ist nämlich klar, dass, wenn D durch kein Quadrat (ausser 1) teilbar ist, es solche Darstellungen überhaupt nicht giebt, dass aber im andern Falle, wenn D durch die Quadrate $\lambda^2, \mu^2, \nu^2, \ldots$ teilbar ist, alle uneigentlichen Darstellungen von D durch F gefunden werden, wenn man sämtliche eigentlichen Darstellungen der Zahlen $\frac{D}{\lambda^2}, \frac{D}{\mu^2}, \frac{D}{\nu^2}, \ldots$ durch dieselbe Form entwickelt und die Werte der Unbestimmten mit $\lambda, \mu, \nu, \ldots$ respective multipliciert.

Auf diese Weise hängt also die Auffindung sämtlicher Darstellungen einer gegebenen Zahl durch eine gegebene ternäre Form, welche irgend einer ternären Formen adjungiert ist, von der zweiten Aufgabe ab; auf diesen Fall aber, der sich auf den ersten Blick nicht soweit zu erstrecken scheinen könnte, lassen sich die übrigen folgendermassen zurückführen. Es sei D die Zahl, welche durch die Form $\begin{pmatrix} g, & g', & g'' \\ h, & h', & h'' \end{pmatrix}$, deren De-

terminante $\triangle$ und der die Form $\begin{pmatrix} G, & G', & G'' \\ H, & H', & H'' \end{pmatrix} = f$ adjungiert ist, dargestellt werden soll. Dann ist der letzteren Form wiederum $\begin{pmatrix} \triangle g, & \triangle g', & \triangle g'' \\ \triangle h, & \triangle h', & \triangle h'' \end{pmatrix} = F$ äquivalent, und es ist klar, dass die Darstellungen der Zahl $\triangle D$ durch F (deren Ermittlung von dem Vorhergehenden abhängt) vollständig identisch sind mit den Darstellungen der Zahl D durch die gegebene Form. — Wenn übrigens sämtliche Coefficienten der Form f einen gemeinschaftlichen Teiler μ haben, so sind augenscheinlich die sämtlichen Coefficienten der Form F durch μ^2 teilbar, weshalb auch $\triangle D$ durch μ^2 teilbar sein muss (sonst würde es keine Darstellungen geben), und die Darstellungen der Zahl D durch die gegebene Form werden identisch sein mit den Darstellungen der Zahl $\frac{\triangle D}{\mu^2}$ durch diejenige Form, welche aus F entsteht, wenn man die einzelnen Coëfficienten mit μ^2 multipliciert, und die derjenigen Form adjungiert ist, welche aus f entsteht, wenn man die einzelnen Coefficienten durch μ dividiert.

Endlich bemerken wir, dass diese Lösung der ersten Aufgabe in dem einen Falle, wo $D = 0$ ist, nicht anwendbar ist, denn in diesem Falle verteilen sich die binären Formen mit der Determinante D nicht auf eine endliche Anzahl von Klassen; weiter unten werden wir diesen Fall aber mit Hülfe anderer Prinzipien erledigen.

282.

Die Ermittlung der Darstellungen einer gegebenen **binären Form**, deren Determinante nicht gleich Null ist,*) durch eine gegebene ternäre Form hängt von folgenden Bemerkungen ab.

I. Aus jeder eigentlichen Darstellung einer binären Form $(p, q, r) = \varphi$ mit der Determinante D durch eine ternäre Form f mit der Determinante $\triangle$ können ganze Zahlen B, B' von solcher Beschaffenheit abgeleitet werden, dass

$$B^2 \equiv \triangle p, \quad BB' \equiv -\triangle q, \quad B'^2 \equiv \triangle r \pmod{D}$$

ist, mit andern Worten, kann der Wert des Ausdrucks $\sqrt{\triangle (p, -q, r)} \pmod{D}$ gefunden werden. Man habe folgende eigentliche Darstellung der Form φ durch f:

$$x = \alpha t + \beta u, \quad x' = \alpha' t + \beta' u, \quad x'' = \alpha'' t + \beta'' u$$

(wo x, x', x''; t, u die Unbestimmten der Formen f, φ bezeichnen); man nehme ganze Zahlen $\gamma, \gamma', \gamma''$ so an, dass

$$(\alpha'\beta'' - \alpha''\beta')\gamma + (\alpha''\beta - \alpha\beta'')\gamma' + (\alpha\beta' - \alpha'\beta)\gamma'' = k$$

*) Diesen Fall $D = 0$, der nach einer etwas verschiedenen Methode zu behandeln ist, übergehen wir hier der Kürze wegen.

entweder gleich $+1$ oder gleich -1 werde, und es gehe f durch die Substitution

$$\begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{matrix}$$

in die Form $\begin{pmatrix} a, a', a'' \\ b, b', b'' \end{pmatrix} = g$ über, welcher die Form $\begin{pmatrix} A, A', A'' \\ B, B', B'' \end{pmatrix} = G$ adjungiert sei. Dann ist klar, dass $a = p$, $b'' = q$, $a' = r$, $A'' = D$ und Δ die Determinante der Form g ist. Daher:

$$B^2 = \Delta p + A'D, \quad BB' = -\Delta q + B''D, \quad B'^2 = \Delta r + AD.$$

So wird z. B. die Form $19t^2 + 6tu + 41u^2$ dargestellt durch $x^2 + x'^2 + x''^2$, wenn man setzt: $x = 3t + 5u$, $x' = 3t - 4u$, $x'' = t$, woraus folgt, wenn man $\gamma = -1$, $\gamma' = 1$, $\gamma'' = 0$ setzt: $B = -171$, $B' = 27$, oder es ist $(-171, 27)$ ein Wert des Ausdrucks $\sqrt{-1\,(19, -3, 41)}$ (mod. 770).

Hieraus folgt bereits, dass, wenn nicht $\Delta\,(p, -q, r)$ quadratischer Rest von D ist, φ durch keine ternäre Form mit der Determinante Δ eigentlich darstellbar sein kann; mithin wird in dem Falle, wo Δ, D prim zu einander sind, Δ die characteristische Zahl der Form φ sein müssen.

II. Da $\gamma, \gamma', \gamma''$ auf unendlich viele Arten bestimmt werden können, so werden daraus auch andere und andere Werte von B, B' sich ergeben, und wir wollen sehen, welchen Zusammenhang sie unter einander haben. Wir nehmen an, dass auch δ, δ', δ'' so beschaffen seien, dass

$$(\alpha'\beta'' - \alpha''\beta')\delta + (\alpha''\beta - \alpha\beta'')\delta' + (\alpha\beta' - \alpha'\beta)\delta'' = \mathfrak{k}$$

entweder gleich $+1$ oder gleich -1 werde, und dass die Form f durch die Substitution

$$\begin{matrix} \alpha, & \beta, & \delta \\ \alpha', & \beta', & \delta' \\ \alpha'', & \beta'', & \delta'' \end{matrix}$$

übergehe in $\begin{pmatrix} \mathfrak{a}, \mathfrak{a}', \mathfrak{a}'' \\ \mathfrak{b}, \mathfrak{b}', \mathfrak{b}'' \end{pmatrix} = \mathfrak{g}$, deren adjungierte $\begin{pmatrix} \mathfrak{A}, \mathfrak{A}', \mathfrak{A}'' \\ \mathfrak{B}, \mathfrak{B}', \mathfrak{B}'' \end{pmatrix} = \mathfrak{G}$ sei. Dann sind g, $\mathfrak{g}$ äquivalent, und daher auch G und $\mathfrak{G}$, und durch Anwendung der in den Artikeln 269, 270 angegebenen Prinzipien findet man, wenn gesetzt wird*):

$$(\beta'\gamma'' - \beta''\gamma')\delta + (\beta''\gamma - \beta\gamma'')\delta' + (\beta\gamma' - \beta'\gamma)\delta'' = \zeta$$
$$(\gamma'\alpha'' - \gamma''\alpha')\delta + (\gamma''\alpha - \gamma\alpha'')\delta' + (\gamma\alpha' - \gamma'\alpha)\delta'' = \eta,$$

*) Indem man aus der Transformation der Form f in g die Transformation von g in f, aus dieser und der Transformation der Form f in $\mathfrak{g}$, die Transformation der Form g in $\mathfrak{g}$, schliesslich aus dieser durch Transposition die Transformation von $\mathfrak{G}$ in G ableitet.

dass $\mathfrak{G}$ in G übergeht durch die Substitution:

$$\begin{matrix} k, & 0, & 0 \\ 0, & k, & 0 \\ \zeta, & \eta, & \mathfrak{k}. \end{matrix}$$

Hiernach ist:

$$B = \eta\mathfrak{k}D + \mathfrak{k}k\mathfrak{B}, \quad B' = \zeta\mathfrak{k}D + \mathfrak{k}kB',$$

und daher wegen $\mathfrak{k}k = \pm 1$ entweder $B \equiv \mathfrak{B}$, $B' \equiv \mathfrak{B}'$ oder $B \equiv -\mathfrak{B}$, $B' \equiv -\mathfrak{B}'$ (mod. D). Im ersten Falle nennen wir die Werte (B, B'), $(\mathfrak{B}, \mathfrak{B}')$ äquivalent, im zweiten entgegengesetzt; von der Darstellung der Form φ aber sagen wir, dass sie zu irgend einem Werte des Ausdrucks $\sqrt{\Delta(p, -q, r)}$ (mod. D), welcher aus ihr nach der Methode in I abgeleitet werden kann, gehöre. Daher werden sämtliche Werte, zu welchem dieselbe Darstellung gehört, entweder äquivalent oder entgegengesetzt sein.

III. Umgekehrt aber, wenn wie vorher in I die folgende Darstellung der Form φ durch f: $x = \alpha t + \beta u, \ldots$ zum Werte (B, B') gehört, welcher daraus mit Hülfe der Transformation

$$\begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{matrix}$$

abgeleitet wird, so wird ebendieselbe auch zu jedem andern Werte $(\mathfrak{B}, \mathfrak{B}')$ gehören, welcher jenem entweder äquivalent oder entgegengesetzt ist, d. h. man kann an Stelle von γ, γ', γ'' andere ganze Zahlen δ, δ', δ'' annehmen, für welche folgende Gleichung (Ω) stattfindet:

$$(\alpha'\beta'' - \alpha''\beta')\delta + (\alpha''\beta - \alpha\beta'')\delta' + (\alpha\beta' - \alpha'\beta)\delta'' = \pm 1,$$

und welche so beschaffen sind, dass der vierte und fünfte Coefficient in der Form, welche derjenigen adjungiert ist, in welche f durch die Substitution (S)

$$\begin{matrix} \alpha, & \beta, & \delta \\ \alpha', & \beta', & \delta' \\ \alpha'', & \beta'', & \delta'' \end{matrix}$$

übergeht, respective gleich $\mathfrak{B}$, $\mathfrak{B}'$ sind. Setzt man nämlich

$$\pm B = \mathfrak{B} + \eta D, \quad \pm B' = \mathfrak{B}' + \zeta D$$

(wo hier und später die oberen oder unteren Zeichen zu nehmen sind, je nachdem die Werte (B, B'), $(\mathfrak{B}, \mathfrak{B}')$ äquivalent sind oder entgegengesetzt), wonach ζ, η ganze Zahlen sind, und geht g durch die Substitution

$$\begin{matrix} 1, & 0, & \zeta \\ 0, & 1, & \eta \\ 0, & 0, & \pm 1 \end{matrix}$$

in die Form $\mathfrak{g}$ über, so sieht man leicht, dass ihre Determinante gleich Δ,

der vierte und fünfte Coefficient in der adjungierten Form aber respective gleich $\mathfrak{B}$, $\mathfrak{B}'$ sind. Macht man aber

$$\alpha\zeta + \beta\eta \pm \gamma = \delta, \quad \alpha'\zeta + \beta'\eta \pm \gamma' = \delta', \quad \alpha''\zeta + \beta''\eta \pm \gamma'' = \delta'',$$

so wird sich ohne Schwierigkeit ergeben, dass f durch die Substitution (S) in $\mathfrak{g}$ übergeht, und dass die Gleichung (Ω) befriedigt ist.

283.

Aus diesen Prinzipien leitet man folgende Methode, sämtliche eigentlichen Darstellungen einer binären Form

$$\varphi = pt^2 + 2qtu + ru^2$$

mit der Determinante D durch die ternäre Form f mit der Determinante Δ zu finden, her.

I. Man ermittle sämtliche verschiedenen (d. h. nicht äquivalenten) Werte des Ausdrucks $\sqrt{\Delta(p, -q, r)}$ (mod. D). Diese Aufgabe ist für den Fall, wo φ eine primitive Form und Δ zu D prim ist, oben (Artikel 233) gelöst, und die übrigen Fälle lassen sich auf diesen sehr leicht zurückführen, was jedoch ausführlicher zu entwickeln die Kürze nicht gestattet. Wir bemerken nur, dass, so oft Δ zu D prim ist, der Ausdruck $\Delta(p, -q, r)$ quadratischer Rest von D nicht sein kann, ausser wenn φ eine primitive Form ist. Denn nehmen wir

$$\Delta p = B^2 - DA', \quad -\Delta q = BB' - DB'', \quad \Delta r = B'^2 - DA$$

an, so wird:

$$(DB'' - \Delta q)^2 = (DA' + \Delta p)(DA + \Delta r)$$

und hieraus, wenn man entwickelt, und $q^2 - pr$ für D setzt:

$$(q^2 - pr)(B''^2 - AA') - \Delta(Ap + 2B''q + A'r) + \Delta^2 = 0,$$

woraus leicht folgt, dass, wenn p, q, r einen gemeinschaftlichen Teiler hätten, derselbe auch in Δ^2 aufgehen würde; dann könnte aber Δ zu D nicht prim sein. Daher können p, q, r keinen gemeinschaftlichen Teiler haben, oder die Form φ ist eine primitive Form.

II. Bezeichnen wir die Anzahl dieser Werte mit m und nehmen wir an, dass sich unter ihnen n Werte finden, die sich selbst entgegengesetzt sind (indem man $n = 0$ setzt, wenn keine solchen vorhanden sind), so ist klar, dass von den $m - n$ übrigen Werten stets je zwei entgegengesetzt sind (da man ja voraussetzt, dass man sämtliche Werte vollständig habe); wird der eine von je zwei beliebigen entgegengesetzten Werten nach Belieben weggelassen, so bleiben im Ganzen $\frac{1}{2}(m + n)$ Werte übrig. So sind z. B. von folgenden acht Werten des Ausdrucks $\sqrt{-1(19, -3, 41)}$ (mod. 770): (39, 237), (171, −27), (269, −83), (291, −127), (−39, −237), (−171, 27), (−269, 83), (−291, 127) die vier letzteren zu verwerfen, weil sie den vier ersteren entgegengesetzt sind. Übrigens ist ersichtlich, dass, wenn (B, B')

ein sich selbst entgegengesetzter Wert ist, $2B$, $2B'$ und somit auch $2\Delta p$, $2\Delta q$, $2\Delta r$ durch D teilbar ist; wenn daher Δ und D prim zu einander sind, so werden auch $2p$, $2q$, $2r$ durch D teilbar sein, und da nach I p, q, r keinen gemeinschaftlichen Teiler haben können, so wird auch 2 durch D teilbar sein müssen, was nur möglich ist, wenn D entweder gleich ± 1 oder gleich ± 2 ist. Daher ist für alle Werte von D, die grösser als 2 sind, stets $n = 0$, falls Δ zu D prim ist.

III. Hiernach ist klar, dass jede eigentliche Darstellung der Form φ durch f notwendig zu irgend einem der übrig bleibenden Werte gehören muss und zwar nur zu einem einzigen. Daher sind diese Werte der Reihe nach zu nehmen und die zu jedem einzelnen gehörigen Darstellungen zu ermitteln. Um die zu einem gegebenen Werte (B, B') gehörigen Darstellungen zu finden, muss man zunächst die ternäre Form $g = \begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$ bestimmen, deren Determinante gleich Δ, und in welcher $a = p$, $b'' = q$, $a' = r$, $ab - b'b'' = B$, $a'b' - bb'' = B'$ ist; die Werte von a'', b, b' findet man hieraus mit Hülfe der Gleichungen im Artikel 276 II, aus denen leicht ersichtlich ist, dass in dem Falle, wo Δ, D prim zu einander sind, b, b', a'' ganze Zahlen werden (weil nämlich diese drei Zahlen, sowohl mit D als mit Δ multipliciert, ganze Zahlen ergeben). Wenn nun entweder einer der Coefficienten b, b', a'' gebrochen ist oder die Formen f, g nicht äquivalent sind, so kann es keine zu (B, B') gehörige Darstellungen der Form φ durch f geben; sind aber b, b', a'' ganze Zahlen und die Formen f, g äquivalent, so liefert jede Transformation jener in diese, wie z. B.

$$\begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha''; & \beta'', & \gamma'' \end{matrix}$$

eine solche Darstellung, nämlich

$$x = \alpha t + \beta u, \quad x' = \alpha' t + \beta' u, \quad x'' = \alpha'' t + \beta'' u,$$

und offenbar kann keine derartige Darstellung existieren, die nicht aus irgend einer Transformation abgeleitet werden könnte. Auf diese Weise ist also derjenige Teil der zweiten Aufgabe, welcher die Aufsuchung der eigentlichen Darstellungen zum Ziele hat, bereits auf die dritte Aufgabe zurückgeführt.

IV. Ferner gehen aus verschiedenen Transformationen der Form f in g immer verschiedene Darstellungen hervor, ausgenommen in dem einzigen Falle, wo der Wert (B, B') sich selbst entgegengesetzt ist, und in dem je zwei Transformationen immer nur eine einzige Darstellung liefern. Nimmt man nämlich an, dass f in g auch durch die Substitution

$$\begin{matrix} \alpha, & \beta, & \delta \\ \alpha', & \beta', & \delta' \\ \alpha'', & \beta'', & \delta'' \end{matrix}$$

(welche dieselbe Darstellung ergiebt wie die vorige Transformation) übergehe und bezeichnet man mit k, $\mathfrak{k}$, ζ, η dieselben Zahlen wie im vorigen Artikel, Abschnitt II, so wird:

$$\mathfrak{B} = k\mathfrak{k}B + \eta\mathfrak{k}D, \quad \mathfrak{B}' = k\mathfrak{k}B' + \zeta\mathfrak{k}D;$$

wenn daher beide Zahlen k, $\mathfrak{k}$, entweder gleich $+1$ oder gleich -1 gesetzt werden, so wird (weil wir den Fall $D = 0$ ausgeschlossen haben) $\zeta = 0$, $\eta = 0$, woraus leicht folgt: $\delta = \gamma$, $\delta' = \gamma'$, $\delta'' = \gamma''$. Daher können jene beiden Transformationen nur in dem einen Falle verschieden sein, wo die eine der Zahlen $\mathfrak{k}$, k gleich $+1$, die andere gleich -1 ist; dann ist $\mathfrak{B} \equiv -B$, $\mathfrak{B}' \equiv -B'$ (mod. D) oder der Wert (B, B') ist sich selbst entgegengesetzt.

V. Aus dem, was wir oben (Artikel 271) über die Kriterien der definiten und indefiniten Formen angegeben haben, folgt leicht, dass, wenn Δ positiv, D negativ und φ eine negative Form ist, g eine definite negative Form wird; dass aber, wenn Δ positiv und entweder D positiv, oder D negativ und φ eine positive Form ist, g eine indefinite Form wird. Da nun f, g sicher nicht äquivalent sein können, wenn sie nicht hinsichtlich dieser Eigenschaft gleichartig sind, so ist klar, dass binäre Formen mit positiver Determinante, sowie positive Formen durch eine ternäre negative Form nicht eigentlich dargestellt werden können, ebenso wenig wie negative binäre Formen durch eine indefinite ternäre Form mit positiver Determinante, sondern vielmehr durch eine ternäre Form der ersten oder zweiten Art einzig und allein binäre Formen der zweiten oder ersten Art respective. Auf ähnliche Weise folgt, dass durch eine definite (d. i. positive) ternäre Form mit negativer Determinante nur positive binäre Formen, durch eine indefinite nur negative binäre Formen mit positiver Determinante dargestellt werden können.

284.

Da die uneigentlichen Darstellungen einer binären Form φ mit der Determinante D durch eine ternäre Form f, welcher die Form F adjungiert ist, diejenigen sind, aus denen sich die uneigentlichen Darstellungen der Zahl D durch die Form F ergeben, so kann offenbar φ durch f nur uneigentlich dargestellt werden, wenn D quadratische Factoren enthält. Nehmen wir an, dass sämtliche in D aufgehende Quadrate (ausser 1) e^2, e'^2, e''^2, ... seien (deren Anzahl endlich ist, da wir voraussetzen, dass D nicht gleich 0 sei), so wird offenbar jede uneigentliche Darstellung der Form φ durch f eine Darstellung der Zahl D durch F liefern, in welcher die Werte der Unbestimmten irgend eine der Zahlen e, e', e'', ... zum grössten gemeinschaftlichen Teiler haben; in dieser Beziehung werden wir der Kürze wegen sagen, dass jede uneigentliche Darstellung der Form φ zum quadratischen Teiler e^2 oder e'^2 oder e''^2 u. s. w. gehöre. Nun werden alle zu demselben gegebenen quadratischen Teiler e^2 (dessen Wurzel e wir als positiv voraussetzen) gehörigen Darstellungen der Form φ durch

folgende Regeln gefunden, aus deren synthetischem Beweis, welcher hier der Kürze wegen vorzuziehen ist, die Analysis, durch welche sie gefunden sind, leicht wiederhergestellt werden kann.

Zuerst ermittle man sämtliche binäre Formen mit der Determinante $\frac{D}{e^2}$, welche in die Form φ durch eine eigentliche Substitution von der Form $T = \varkappa t + \lambda u$, $U = \mu u$ übergehen, wo T, U die Unbestimmten einer solchen Form, t, u die Unbestimmten der Form φ, $\varkappa$, μ positive ganze Zahlen (deren Product somit gleich e ist) und λ eine positive ganze Zahl bezeichnen, die kleiner als μ ist (einschliesslich der Null). Diese Formen nebst den entsprechenden Transformationen werden folgendermassen gefunden:

Man setze $\varkappa$ der Reihe nach gleich den einzelnen positiv genommenen Teilern von e (1 und e mit eingeschlossen) und es werde $\mu = \frac{e}{\varkappa}$ gemacht; für die einzelnen bestimmten Werte von $\varkappa$, μ lege man λ sämtliche ganzen Werte von 0 bis $\mu - 1$ bei, wodurch man sicher alle Transformationen erhält. Dann findet man die Form, welche durch jede Substitution $T = \varkappa t + \lambda u$, $U = \mu u$ in φ übergeht, indem man die Form sucht, in welche φ durch die Substitution $t = \frac{1}{\varkappa} T - \frac{\lambda}{e} U$, $u = \frac{1}{\mu} U$ übergeht; auf diese Weise erhält man die den einzelnen Transformationen entsprechenden Formen; aber von allen diesen Formen sind nur die beizubehalten, in denen alle drei Coefficienten ganze Zahlen werden*).

Zweitens nehme an, dass Φ irgend eine von diesen Formen sei, welche in φ durch die Substitution $T = \varkappa t + \lambda u$, $U = \mu u$ übergehen möge, ermittele alle eigentlichen Darstellungen der Form Φ durch f (wenn es deren giebt) und stelle sie unbestimmt durch

$$(\mathfrak{R})\qquad x = \mathfrak{A}T + \mathfrak{B}U,\quad x' = \mathfrak{A}'T + \mathfrak{B}'U,\quad x'' = \mathfrak{A}''T + \mathfrak{B}''U$$

dar; endlich leite man aus den einzelnen Darstellungen (R) die Darstellung

$$(\rho)\qquad x = \alpha t + \beta u,\qquad x' = \alpha' t + \beta' u,\qquad x'' = \alpha'' t + \beta'' u$$

mittelst der Gleichungen

$$(R)\qquad \begin{matrix} \alpha = \varkappa\mathfrak{A}, & \alpha' = \varkappa\mathfrak{A}', & \alpha'' = \varkappa\mathfrak{A}'' \\ \beta = \lambda\mathfrak{A} + \mu\mathfrak{B}, & \beta' = \lambda\mathfrak{A}' + \mu\mathfrak{B}', & \beta'' = \lambda\mathfrak{A}'' + \mu\mathfrak{B}'' \end{matrix}$$

ab. Auf ganz dieselbe Weise wie die Form Φ behandle man die übrigen nach der ersten Regel gefundenen Formen (wenn mehrere vorhanden sind),

*) Wenn wir hier über dieses Problem ausführlicher handeln könnten, würden wir die Lösung beträchtlich zusammenziehen können. Das ist ohne Weiteres klar, dass man für $\varkappa$ andere Teiler von e nicht zu nehmen braucht, als solche, deren Quadrat in dem ersten Coefficienten der Form φ aufgeht. Übrigens behalten wir uns vor, dieses Problem, aus dem auch einfachere Lösungen des Problems im Artikel 213, 214 abgeleitet werden können, bei anderer passender Gelegenheit wieder aufzunehmen.

so dass aus den einzelnen eigentlichen Darstellungen einer jeden andere Darstellungen abgeleitet werden, dann werden, wie ich behaupte, auf diese Weise sämtliche zum Teiler e^2 gehörige Darstellungen der Form φ, und zwar jede nur einmal hervorgehen.

Beweis. I. Dass die ternäre Form f durch jede Substitution (ρ) wirklich in φ übergeht, ist so klar, dass es einer weiteren Auseinandersetzung nicht bedarf; dass aber jede Darstellung (ρ) eine uneigentliche ist und zum Teiler e^2 gehört, geht daraus hervor, dass die Zahlen $\alpha'\beta''-\alpha''\beta'$, $\alpha''\beta-\alpha\beta''$, $\alpha\beta'-\alpha'\beta$ respective gleich $e(\mathfrak{A}'\mathfrak{B}''-\mathfrak{A}''\mathfrak{B}')$, $e(\mathfrak{A}''\mathfrak{B}-\mathfrak{A}\mathfrak{B}'')$, $e(\mathfrak{A}\mathfrak{B}'-\mathfrak{A}'\mathfrak{B})$ werden, wonach offenbar ihr grösster gemeinschaftlicher Teiler e ist (da $(\mathfrak{R})$ eine eigentliche Darstellung ist).

II. Wir werden zeigen, dass aus jeder gegebenen Darstellung (ρ) der Form φ eine eigentliche Darstellung der Form mit der Determinante $\frac{D}{e^2}$, welche unter den nach der ersten Regel gefundenen Darstellungen enthalten ist, gefunden werden kann, oder dass aus gegebenen Werten von $\alpha, \alpha', \alpha''$, β, β', β'' ganzzahlige Werte von $\varkappa, \lambda, \mu$, welche den vorgeschriebenen Bedingungen, und Werte von $\mathfrak{A}, \mathfrak{A}', \mathfrak{A}'', \mathfrak{B}, \mathfrak{B}', \mathfrak{B}''$, welche den Gleichungen (R) genügen, abgeleitet werden können und zwar nur auf eine einzige Weise. Denn zunächst geht aus den ersten drei Gleichungen in (R) hervor, dass für $\varkappa$ der grösste gemeinschaftliche Teiler von $\alpha, \alpha', \alpha''$ mit positivem Vorzeichen genommen werden muss (da nämlich $\mathfrak{A}'\mathfrak{B}''-\mathfrak{A}''\mathfrak{B}'$, $\mathfrak{A}''\mathfrak{B}-\mathfrak{A}\mathfrak{B}''$, $\mathfrak{A}\mathfrak{B}'-\mathfrak{A}'\mathfrak{B}$ keinen gemeinschaftlichen Teiler haben, so können auch $\mathfrak{A}, \mathfrak{A}', \mathfrak{A}''$ einen gemeinschaftlichen Teiler nicht haben); dadurch sind auch $\mathfrak{A}, \mathfrak{A}', \mathfrak{A}''$ bestimmt und ebenso $\mu=\frac{e}{\varkappa}$ (dass diese Zahl notwendig eine ganze Zahl ist, sieht man leicht). Nehmen wir an, dass drei ganze Zahlen $\mathfrak{a}, \mathfrak{a}', \mathfrak{a}''$ so angenommen seien, dass $\mathfrak{a}\mathfrak{A}+\mathfrak{a}'\mathfrak{A}'+\mathfrak{a}''\mathfrak{A}''=1$ wird, und schreiben wir der Kürze wegen k für $\mathfrak{a}\mathfrak{B}+\mathfrak{a}'\mathfrak{B}'+\mathfrak{a}''\mathfrak{B}''$, so folgt aus den drei letzten Gleichungen (R), dass $\mathfrak{a}\beta+\mathfrak{a}'\beta'+\mathfrak{a}''\beta''=\lambda+\mu k$ ist, woraus sofort hervorgeht, dass es für λ nur einen einzigen Wert zwischen 0 und $\mu-1$ giebt. Da nun, nachdem dies geschehen, auch $\mathfrak{B}, \mathfrak{B}', \mathfrak{B}''$ bestimmte Werte erhalten, so haben wir nur noch zu beweisen, dass diese stets ganz sind. Es wird aber:

$$\begin{aligned}\mathfrak{B}=\frac{1}{\mu}(\beta-\lambda\mathfrak{A})&=\frac{1}{\mu}[\beta\ (1-\mathfrak{a}\mathfrak{A}) \quad -\mathfrak{A}(\mathfrak{a}'\beta'+\mathfrak{a}''\beta'')]+\mathfrak{A}k\\ &=\frac{1}{\mu}[\mathfrak{a}''(\mathfrak{A}''\beta-\mathfrak{A}\beta'')-\mathfrak{a}'(\mathfrak{A}\beta'-\mathfrak{A}'\beta\ )]+\mathfrak{A}k\\ &=\frac{1}{e}[\mathfrak{a}''(\alpha''\beta-\alpha\beta'')\ -\mathfrak{a}'(\alpha\beta'-\alpha'\beta\ )]+\mathfrak{A}k,\end{aligned}$$

und es ist daher $\mathfrak{B}$ offenbar eine ganze Zahl, und ebenso bestätigt man, dass auch $\mathfrak{B}', \mathfrak{B}''$ ganzzahlige Werte erhalten. — Aus dieser Schlussreihe ergiebt sich, dass es keine uneigentliche, zum Teiler e^2 gehörige Dar-

stellung der Form φ durch f geben kann, welche man durch die angegebene Methode entweder nicht oder mehrere Male erhalten könnte.

Wenn man nun in derselben Weise die übrigen quadratischen Teiler von D behandelt und die zu jedem einzelnen gehörigen Darstellungen ermittelt, so erhält man sämtliche uneigentlichen Darstellungen der Form φ durch f.

Ferner ergiebt sich aus dieser Lösung leicht, dass das am Schlusse des vorigen Artikels für die eigentlichen Darstellungen angegebene Theorem auch für die uneigentlichen gilt, nämlich dass allgemein keine positive binäre Form mit negativer Determinante durch eine negative ternäre Form dargestellt werden kann, u. s. w. Denn offenbar werden, wenn φ eine solche binäre Form ist, welche jenem Satze zufolge durch f nicht eigentlich dargestellt werden kann, auch alle Formen mit den Determinanten $\frac{D}{e^2}, \frac{D}{e'^2}, \ldots,$ welche φ enthalten, durch f nicht eigentlich dargestellt werden können, da alle diese Formen eine Determinante haben, welche dasselbe Vorzeichen hat wie φ und, wenn diese Determinanten negativ sind, entweder sämtlich positive oder sämtlich negative Formen werden, je nachdem φ zu jenen oder zu diesen gehört.

285.

Über die Fragen, welche das dritte uns gestellte Problem bilden (auf welches im Vorhergehenden die beiden ersten zurückgeführt sind), nämlich wenn zwei ternäre Formen mit derselben Determinante gegeben sind, zu entscheiden, ob sie äquivalent sind oder nicht, und im ersteren Falle alle Transformationen der einen in die andere zu finden, können wir an dieser Stelle nur wenig anführen, da die vollständige Lösung, die wir für die analogen Probleme bei binären Formen angegeben haben, hier noch grösseren Schwierigkeiten unterliegt. Daher beschränken wir unsere Untersuchung auf gewisse specielle Fälle, derentwegen wir hauptsächlich diese Abschweifung von unserm eigentlichen Gegenstande gemacht haben.

I. Es ist oben gezeigt worden, dass für die Determinante $+1$ alle ternären Formen in zwei Klassen zerfallen, von denen die eine alle indefiniten Formen, die andere alle definiten (negativen) Formen enthält. Hieraus folgt sogleich, dass zwei beliebige ternäre Formen mit der Determinante 1 äquivalent sind, wenn entweder beide definit oder beide indefinit sind; dass aber, wenn die eine definit, die andere indefinit ist, eine Äquivalenz nicht stattfinden kann (der erste Teil des Satzes gilt offenbar allgemein für Formen mit irgend welcher Determinante). — Ebenso werden irgend zwei Formen mit der Determinante -1 sicher äquivalent sein, wenn entweder beide definit, oder beide indefinit sind. — Zwei definite Formen mit der Determinante 2 werden stets äquivalent sein; zwei indefinite werden nicht äquivalent sein, wenn in der einen die drei ersten Coefficienten sämtlich gerade, in der andern aber nicht sämtlich gerade sind; in den übrigen Fällen (wenn

entweder jede oder keine der beiden Formen drei gleichzeitig gerade erste Coefficienten hat) werden sie dagegen äquivalent sein. — Auf diese Weise könnten wir noch weit mehr specielle Sätze aufstellen, wenn wir oben (Artikel 277) mehr Beispiele entwickelt hätten.

II. Für alle diese Fälle kann man auch, wenn f, f' ternäre äquivalente Formen bezeichnen, eine Transformation der einen in die andere finden. Denn für alle Fälle ist in jeder Klasse der ternären Formen eine hinreichend kleine Anzahl von Formen oben angegeben worden, auf deren irgend eine jede Form derselben Klasse vermittelst einförmiger Methoden zurückgeführt werden kann; wie man alle diese auf eine einzige reducieren kann, ist ebendaselbst gezeigt werden. Ist F diese Form in derjenigen Klasse, zu welcher f, f' gehören, so können nach den oben angegebenen Regeln die Transformationen von f, f' in F und ebenso auch die von F in f, f' gefunden werden. Hieraus können nach Artikel 270 die Transformationen der Form f in f' und der Form f' in f abgeleitet werden.

III. Es bleibt daher nur übrig zu zeigen, wie man aus einer Transformation einer ternären Form f in eine andere f' alle möglichen Transformationen ableiten kann. Diese Aufgabe hängt von der einfacheren ab, alle Transformationen einer ternären Form f **in sich selbst** zu finden. Wenn nämlich f durch mehrere Substitutionen (τ), (τ'), (τ''), ... in sich selbst und durch die Substitution (t) in f' übergeht, so werden offenbar, wenn man nach der Vorschrift des Artikels 270 die Transformation (t) mit (τ), (τ'), (τ''), ... combiniert, Transformationen sich ergeben, durch welche sämtlich f in f' übergeht; überdies bestätigt man durch Rechnung leicht, dass jede Transformation der Form f in f' auf diese Weise abgeleitet werden kann aus einer Combination der gegebenen Transformation (t) der Form f in f' mit einer (und zwar nur einer) Transformation der Form f in sich selbst, und dass somit aus der Combination einer gegebenen Transformation der Form f in f' mit sämtlichen Transformationen der Form f in sich selbst sämtliche Transformationen der Form f in f', und zwar die einzelnen nur einmal, hervorgehen.

Die Ermittlung sämtlicher Transformationen der Form f in sich selbst beschränken wir hier auf den Fall, wo f eine definite Form ist, in welcher der vierte, fünfte und sechste Coefficient sämtlich gleich 0 sind.*) Es sei daher $f = \begin{pmatrix} a, & a', & a'' \\ 0, & 0, & 0 \end{pmatrix}$, und es mögen alle Substitutionen, durch welche f in sich selbst übergeht, unbestimmt durch

$$\begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{matrix}$$

*) Die übrigen Fälle, in denen f eine definite Form ist, lassen sich auf diesen zurückführen; ist aber f eine indefinite Form, so ist eine ganz verschiedene Methode anzuwenden und die Anzahl der Transformationen ist unendlich gross.

dargestellt werden, so dass man den Gleichungen genügen muss:

$$(\Omega)\qquad \begin{aligned} a\alpha^2 + a'\alpha'^2 + a''\alpha''^2 &= a\\ a\beta^2 + a'\beta'^2 + a''\beta''^2 &= a'\\ a\gamma^2 + a'\gamma'^2 + a''\gamma''^2 &= a''\\ a\alpha\beta + a'\alpha'\beta' + a''\alpha''\beta'' &= 0\\ a\alpha\gamma + a'\alpha'\gamma' + a''\alpha''\gamma'' &= 0\\ a\beta\gamma + a'\beta'\gamma' + a''\beta''\gamma'' &= 0. \end{aligned}$$

Nun sind drei Fälle zu unterscheiden.

I. Sind a, a', a'' (welche dasselbe Vorzeichen haben) sämtlich von einander verschieden, so nehmen wir an, dass $a < a'$, $a' < a''$ sei (Sollte eine andere Reihenfolge in der Grösse stattfinden, so lassen sich dieselben Schlüsse auf ganz analoge Weise ableiten). Dann erfordert die erste Gleichung in (Ω) offenbar, dass $\alpha' = \alpha'' = 0$ und daher $\alpha = \pm 1$ sei; hierauf wird aus der vierten und fünften Gleichung $\beta = 0$, $\gamma = 0$; ähnlich aus der zweiten Gleichung $\beta'' = 0$ und somit $\beta = \pm 1$ und sodann aus der sechsten Gleichung $\gamma' = 0$ und aus der dritten $\gamma'' = \pm 1$, so dass man (wegen der von einander unabhängigen doppelten Vorzeichen) acht verschiedene Transformationen erhält.

II. Wenn von den Zahlen a, a', a'' zwei, z. B. $a' = a''$, einander gleich, die dritte aber verschieden ist, so nehmen wir an

Erstens $a < a'$. Dann wird in derselben Weise wie im vorigen Falle $\alpha' = 0$, $\alpha'' = 0$, $\alpha = \pm 1$, $\beta = 0$, $\gamma = 0$; aus der zweiten, dritten und sechsten Gleichung aber folgt leicht, dass entweder $\beta' = \pm 1$, $\gamma' = 0$, $\beta'' = 0$, $\gamma'' = \pm 1$, oder $\beta' = 0$, $\gamma' = \pm 1$, $\beta'' = \pm 1$, $\gamma'' = 0$ ist.

Ist aber zweitens $a > a'$, so erhält man dieselben Schlüsse folgendermassen: Aus der zweiten und dritten Gleichung ist notwendig: $\beta = 0$, $\gamma = 0$ und entweder $\beta' = \pm 1$, $\gamma' = 0$, $\beta'' = 0$, $\gamma'' = \pm 1$, oder $\beta' = 0$, $\gamma' = \pm 1$, $\beta'' = \pm 1$, $\gamma'' = 0$. Für beide Annahmen folgt aus der vierten und fünften Gleichung $\alpha' = 0$, $\alpha'' = 0$ und aus der ersten $\alpha = \pm 1$. Man hat daher für jeden Fall sechzehn verschiedene Transformationen. — Die beiden andern Fälle, in denen entweder $a = a''$ oder $a = a'$ ist, werden in ganz analoger Weise erledigt, wenn man nur die Buchstaben $\alpha, \alpha', \alpha''$ im ersten Falle mit β, β', β'', im zweiten mit $\gamma, \gamma', \gamma''$ respective vertauscht.

III. Wenn alle drei Zahlen a, a', a'' einander gleich sind, so erfordern die drei ersten Gleichungen, dass von den drei Zahlen $\alpha, \alpha', \alpha''$, ebenso von β, β', β'' und von $\gamma, \gamma', \gamma''$ je zwei gleich 0, die dritte gleich ± 1 sei. Aus den drei letzten Gleichungen aber erkennt man leicht, dass von den drei Zahlen α, β, γ nur eine gleich ± 1 sein kann, und ebenso bei α', β', γ' und $\alpha'', \beta'', \gamma''$. Daher giebt es nur sechs Combinationen:

α	α	α'	α'	α''	α''	$= \pm 1$	
β'	β''	β	β''	β	β'	$= \pm 1$	; die übrigen sechs Coefficienten $= 0$,
γ''	γ'	γ''	γ	γ'	γ	$= \pm 1$	

so dass man wegen der doppelten Vorzeichen im Ganzen 48 Transformationen erhält. — Dasselbe Schema umfasst auch die vorhergehenden Fälle; man hat aber von den sechs ersten Kolonnen nur die erste zu nehmen, wenn a, a', a'' alle ungleich sind; die erste und zweite Kolonne, wenn $a' = a''$, die erste und dritte, wenn $a = a'$, und die erste und sechste, wenn $a = a''$ ist.

Hieraus ergiebt sich, dass, wenn die ternäre Form $f = ax^2 + a'x'^2 + a''x''^2$ in eine andere äquivalente Form f' übergeht durch die Substitution:

$$x = \delta y + \varepsilon y' + \zeta y'', \quad x' = \delta' y + \varepsilon' y' + \zeta' y'', \quad x'' = \delta'' y + \varepsilon'' y' + \zeta'' y'',$$

sämtliche Transformationen der Form f in f' enthalten sind unter folgendem Schema:

x	x	x'	x'	x''	x''	$= \pm(\delta y + \varepsilon y' + \zeta y'')$
x'	x''	x	x''	x	x'	$= \pm(\delta' y + \varepsilon' y' + \zeta' y'')$
x''	x'	x''	x	x'	x	$= \pm(\delta'' y + \varepsilon'' y' + \zeta'' y'')$,

mit der Massgabe, dass alle sechs ersten Kolonnen anzuwenden sind, wenn $a = a' = a''$ ist, die erste und zweite Kolonne, wenn a', a'' einander gleich, a verschieden ist, die erste und dritte, wenn $a = a'$, die erste und sechste, wenn $a = a''$, endlich die erste Kolonne allein, wenn a, a', a'' sämtlich von einander verschieden sind. Im ersten Falle ist die Anzahl der Transformationen gleich 48, im zweiten, dritten und vierten gleich 16 und im fünften gleich 8.

Gewisse Anwendungen auf die Theorie der binären Formen.

Über die Ermittlung der Form, aus deren Duplikation eine gegebene binäre Form des Hauptgeschlechts entsteht.

Von dieser kurzen Auseinandersetzung der ersten Elemente der Theorie der ternären Formen gehen wir zu gewissen speciellen Anwendungen über, unter denen das folgende Problem den ersten Platz verdient.

286.

Aufgabe. Wenn eine zum Hauptgeschlechte gehörige binäre Form $F = (A, B, C)$ mit der Determinante D gegeben ist, so soll man die binäre Form f finden, durch deren Duplikation jene entsteht.

Auflösung. I. Man suche eine eigentliche Darstellung der zu F entgegengesetzten Form $F' = AT^2 - 2BTU + CU^2$ durch die ternäre Form $x^2 - 2yz$, und zwar sei dieselbe:

$$x = \alpha T + \beta U, \quad y = \alpha' T + \beta' U, \quad z = \alpha'' T + \beta'' U.$$

Dass dies möglich ist, ergiebt sich leicht aus der vorstehenden Theorie der ternären Formen. Denn da nach Voraussetzung F aus dem Hauptgeschlechte ist, so giebt es einen Wert des Ausdrucks $\sqrt{(A, B, C)}$ (mod. D), wonach eine ternäre Form φ mit der Determinante 1 gefunden werden kann, in welche $(A, -B, C)$ als Teil eingeht, und man erkennt leicht, dass sämtliche Coefficienten dieser Form ganze Zahlen sind. Ebenso leicht sieht man, dass φ eine indefinite Form ist (da F nach Voraussetzung sicher keine negative Form ist); daher ist sie notwendig der Form $x^2 - 2yz$ äquivalent. Man kann daher eine Transformation dieser in jene bestimmen, welche eine eigentliche Darstellung der Form F durch $x^2 - 2yz$ liefert. — Alsdann ist also:

$$A = \alpha^2 - 2\alpha'\alpha'', \quad -B = \alpha\beta - \alpha'\beta'' - \alpha''\beta', \quad C = \beta^2 - 2\beta'\beta'';$$

bezeichnet man ferner die Zahlen $\alpha\beta' - \alpha'\beta$, $\alpha'\beta'' - \alpha''\beta'$, $\alpha''\beta - \alpha\beta''$ mit a, b, c respective, so werden diese keinen gemeinschaftlichen Teiler haben, und es ist $D = b^2 - 2ac$.

II. Hieraus folgert man mit Hülfe der letzten Bemerkung im Artikel 235 leicht, dass F durch die Substitution $2\beta', \beta, \beta, \beta''$; $2\alpha', \alpha, \alpha, \alpha''$ in das Product der Form $(2a, -b, c)$ mit sich selbst, ebenso durch die Substitution $\beta', \beta, \beta, 2\beta''$; $\alpha', \alpha, \alpha, 2\alpha''$ in das Product der Form $(a, -b, 2c)$ mit sich selbst übergeht. Nun ist der grösste gemeinschaftliche Teiler der Zahlen $2a$, $2b$, $2c$ gleich 2; wenn daher c ungerade ist, so werden $2a$, $2b$, c keinen gemeinschaftlichen Teiler haben, oder $(2a, -b, c)$ wird eine eigentlich primitive Form sein; ebenso ist, wenn a ungerade ist, $(a, -b, 2c)$ eine eigentlich primitive Form. Im ersten Falle entsteht F durch Duplikation der Form $(2a, -b, c)$, im zweiten durch Duplikation der Form $(a, -b, 2c)$ (Vgl. die vierte Folgerung im Artikel 235); einer von diesen Fällen aber wird sicher immer stattfinden. Denn wenn beide Zahlen a, c gerade wären, würde b notwendig ungerade sein; nun bestätigt man leicht, dass $\beta''a + \beta b + \beta'c = 0$, $\alpha''a + \alpha b + \alpha'c = 0$ ist, woraus folgen würde, dass βb, αb und daher auch α und β gerade wären. Hiernach aber würden A und C gerade sein, was gegen die Voraussetzung wäre, nach welcher F eine Form aus dem Hauptgeschlechte und daher aus einer eigentlich primitiven Ordnung ist. — Übrigens ist es auch möglich, dass a und c ungerade sind, in welchem Falle man somit gleich zwei Formen hat, durch deren Duplikation F entsteht.

Beispiel. Es sei die Form $F = (5, 2, 31)$ mit der Determinante -151 gegeben. Als Wert des Ausdrucks $\sqrt{(5, 2, 31)}$ findet man hier $(55, 22)$ und hieraus die ternäre Form $\varphi = \begin{pmatrix} 5, & 31, & 4 \\ 11, & 0, & -2 \end{pmatrix}$; nach den Regeln im Artikel 272 findet man die zu dieser äquivalente Form $\begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$, welche in φ übergeht durch die Substitution $\begin{Bmatrix} 2, & 2, & 1 \\ 1, & -6, & -2 \\ 0, & 3, & 1 \end{Bmatrix}$. Hieraus folgt mittelst der im

Artikel 277 angegebenen Transformationen, dass $\begin{pmatrix} 1, 0, 0 \\ -1, 0, 0 \end{pmatrix}$ in φ übergeht durch die Substitution $\begin{Bmatrix} 3, -7, -2 \\ 2, -1, 0 \\ 1, -9, -3 \end{Bmatrix}$. Es wird daher $a = 11$, $b = -17$, $c = 20$; mithin entsteht F, da a ungerade ist, durch Duplikation der Form $(11, 17, 40)$ und geht in das Produkt dieser Form mit sich selbst über durch die Substitution $-1, -7, -7, -18;\ 2, 3, 3, 2$.

Allen Characteren mit Ausnahme derjenigen, welche in den Artikeln 263, 264 als unmöglich gefunden worden sind, entsprechen wirklich Geschlechter.

287.

In Bezug auf die im vorigen Artikel gelöste Aufgabe fügen wir noch folgende Bemerkungen hinzu.

I. Wenn die Form F durch die Substitution p, p', p'', p'''; q, q', q'', q''' in das Product der beiden Formen (h, i, k), (h', i', k') übergeht (jede der beiden, wie wir stets voraussetzen, eigentlich genommen), so hat man die aus der dritten Folgerung in Artikel 235 leicht ableitbaren Gleichungen:

$$p''hn' - p'h'n - p(in' - i'n) = 0$$
$$(p'' - p')(in' + i'n) - p(kn' - k'n) + p'''(hn' - h'n) = 0$$
$$p'kn' - p''k'n - p'''(in' - i'n) = 0,$$

und drei andere, welche aus diesen durch Vertauschung der Zahlen p, p', p'', p''' mit q, q', q'', q''' entstehen; n, n' sind die positiven Quadratwurzeln aus den Quotienten, welche man erhält, wenn man die Determinanten der Formen (h, i, k), (h', i', k') durch die Determinante der Form F dividiert. Wenn daher diese Formen identisch sind, oder $n = n'$, $h = h'$, $i = i'$, $k = k'$ ist, so gehen jene Gleichungen in die folgenden über:

$$(p'' - p')hn = 0, \quad (p'' - p')in = 0, \quad (p'' - p')kn = 0,$$

woraus notwendig $p' = p''$ und auf ganz ähnliche Weise $q' = q''$ sich ergiebt. — Giebt man also den Formen (h, i, k), (h', i', k') dieselben Unbestimmten t, u und bezeichnet man die Unbestimmten der Form F mit T, U, so wird F durch die Substitution

$$T = pt^2 + 2p'tu + p'''u^2, \quad U = qt^2 + 2q'tu + q'''u^2$$

in $(ht^2 + 2itu + ku^2)^2$ übergehen.

II. Wenn die Form F durch Duplikation der Form f entsteht, so wird sie auch durch Duplikation jeder andern mit f in derselben Klasse enthaltenen Form oder die Klasse der Form F durch Duplikation der Klasse der Form f entstehen (Vgl. Artikel 238). So entsteht bei dem Beispiel des vorigen Artikels die Form $(5, 2, 31)$ auch durch Duplikation der Form

(11, —5, 16), welche der Form (11, 17, 40) eigentlich äquivalent ist. Aus der einen Klasse, durch deren Duplikation die Klasse der Form F entsteht, findet man alle (wenn es mehrere giebt) mittelst der Aufgabe im Artikel 260; in unserem Beispiele giebt es keine andere positive Klasse dieser Art, da nur eine ambige eigentlich primitive positive Klasse mit der Determinante — 151 existiert (nämlich die Hauptklasse); da durch Composition der einzigen ambigen negativen Klasse (—1, 0, —151) mit der Klasse (11, —5, 16) die Klasse (—11, —5, —16) entsteht, so wird diese die einzige negative Klasse sein, aus deren Duplikation die Klasse (5, 2, 31) hervorgeht.

III. Da durch die Auflösung der Aufgabe des vorigen Artikels selbst festgestellt wird, dass jede eigentlich primitive (positive) zum Hauptgeschlechte gehörige Klasse binärer Formen aus der Duplikation irgend einer eigentlich primitiven Klasse mit derselben Determinante entstehen kann, so lässt sich der Satz des Artikels 261, durch welchen wir die Gewissheit erhielten, dass wenigstens der Hälfte aller für eine gegebene nichtquadratische Determinante D möglichen Charactere keine eigentlich primitiven (positiven) Geschlechter entsprechen können, nunmehr dahin erweitern, dass in der That genau der Hälfte aller dieser Charactere derartige Geschlechter entsprechen, der anderen Hälfte somit keine solchen Geschlechter entsprechen können (Vgl. den Beweis jenes Satzes). Somit ist jetzt, da im Artikel 264 alle jene möglichen Charactere in zwei Arten P, Q gleichmässig verteilt sind, von denen die letzteren Q, wie bewiesen worden ist, eigentlich primitiven (positiven) Formen nicht entsprechen können, während es in Bezug auf die übrigen P zweifelhaft blieb, ob den einzelnen stets wirklich solche Geschlechter entsprechen, dieser Zweifel vollständig gehoben und wir sind sicher, dass in dem ganzen Complex von Characteren P keiner vorhanden ist, welchem ein Geschlecht nicht entspräche. — Hieraus leitet man auch leicht her, dass für eine negative Determinante in einer negativen eigentlich primitiven Ordnung, in welcher, wie wir im Artikel 264, I gezeigt haben, alle P unmöglich und nur allein die Q möglich sind, auch wirklich alle Q möglich sind. Bezeichnet nämlich K irgend einen Character aus Q, f eine beliebige Form aus der negativen eigentlich primitiven Ordnung der Formen mit der Determinante D und K' ihren Character, so wird derselbe aus Q sein, woraus leicht folgt, dass der aus K, K' (nach der Vorschrift des Artikels 246) zusammengesetzte Character zu P gehört, und dass es somit positive eigentlich primitive Formen mit der Determinante D giebt, welche demselben entsprechen; durch Composition einer solchen Form mit f entsteht offenbar eine negative eigentlich primitive Form mit der Determinante D, deren Character K ist. — Auf ganz analoge Weise zeigt man, dass in einer uneigentlich primitiven Ordnung diejenigen Charactere, welche nach den Regeln des Artikels 264, II, III als allein mögliche gefunden werden, sämtlich möglich sind, mögen sie zu den P oder zu den Q gehören. — Diese Sätze sind, wenn wir nicht sehr irren, zu den schönsten in der Theorie der binären Formen zu rechnen,

umsomehr weil sie, obwohl sie höchst einfacher Natur sind, doch so versteckt liegen, dass man einen strengen Beweis derselben ohne Unterstützung durch so viele andere Untersuchungen nicht zu erbringen vermag.

Theorie der Zerlegung sowohl der Zahlen wie der binären Formen in drei Quadrate.

Wir gehen jetzt zu einer anderen Anwendung der vorhergehenden Digression, nämlich zur Zerlegung sowohl der Zahlen als auch der binären Formen in drei Quadrate, über und schicken derselben folgende Aufgabe voraus.*)

288.

Aufgabe. Bezeichnet M eine positive Zahl, so soll man die Bedingungen finden, unter denen es negative primitive binäre Formen mit der Determinante $-M$ geben kann, welche quadratische Reste von M sind, oder für welche 1 die characteristische Zahl ist.

Auflösung. Wir bezeichnen mit Ω den Complex aller Specialcharactere, welche die Beziehungen der Zahl 1 sowohl zu den einzelnen (ungeraden) Primteilern von M als auch zu der Zahl 8 oder 4, wenn sie in M aufgehen, angeben; offenbar werden diese Charactere Rp, Rp', Rp'', ..., wo p, p', p'', ... jene Primteiler bezeichnen, und 1, 4, falls 4, dagegen 1, 8 sein, falls 8 in M aufgeht. Ferner bedienen wir uns der Buchstaben P, Q in derselben Bedeutung wie im vorigen Artikel oder wie im Artikel 264. Wir unterscheiden nun die folgenden Fälle:

I. Ist M durch 4 teilbar, so ist Ω ein Totalcharacter und aus Artikel 233. V geht hervor, dass 1 nur von solchen Formen characteristische Zahl sein kann, deren Character Ω ist. Offenbar aber ist Ω der Character der Hauptform $(1, 0, M)$ und gehört somit zu P, kann also nicht einer negativen eigentlich primitiven Form zukommen; daher giebt es, weil es uneigentlich primitive Formen für eine solche Determinante nicht giebt, in diesem Falle überhaupt keine negativen primitiven Formen, welche Reste von M sind.

II. Ist $M \equiv 3 \pmod{4}$, so gelten genau dieselben Schlüsse mit der einzigen Ausnahme, dass in diesem Falle eine uneigentlich primitive negative Ordnung existiert, in welcher die Charactere P entweder möglich oder unmöglich sind, je nachdem $M \equiv 3$ oder $\equiv 7 \pmod{8}$ ist. Vgl. Artikel 264, III. Im ersten Falle giebt es also in dieser Ordnung ein Geschlecht, dessen Character Ω ist, weshalb 1 die characteristische Zahl aller in ihm enthaltenen Formen ist; im zweiten Falle kann es überhaupt keine negativen Formen geben, welche diese Eigenschaft besitzen.

III. Ist $M \equiv 1 \pmod{4}$, so ist Ω noch kein Totalcharacter, vielmehr muss noch die Beziehung zur Zahl 4 hinzukommen; offenbar aber muss Ω

*) Vgl. die Zusätze am Schlusse der *Disquisitiones*.

notwendig in den Character der Form, deren characteristische Zahl 1 ist, eingehen, und umgekehrt muss jede Zahl, deren Character entweder Ω; 1, 4 oder Ω; 3, 4 ist, die characteristische Zahl 1 haben. Nun ist Ω; 1, 4 offenbar der Character des Hauptgeschlechts, welcher zu P gehört und daher in der negativen eigentlich primitiven Ordnung unmöglich ist; aus demselben Grunde gehört Ω; 3, 4 zu Q (Artikel 263), weshalb ihm in der negativen eigentlich primitiven Ordnung ein Geschlecht entspricht, dessen Formen sämtlich die characteristische Zahl 1 haben. Eine uneigentlich primitive Ordnung giebt es in diesem Falle nicht, ebensowenig in dem folgenden.

IV. Ist $M \equiv 2$ (mod. 4), so muss zu Ω die Relation zu 8, durch welche es ein Totalcharacter wird, nämlich entweder 1 u. 3, 8 oder 5 u. 7, 8, falls $M \equiv 2$ (mod. 8) und entweder 1 u. 7, 8 oder 3 u. 5, 8, falls $M \equiv 6$ (mod. 8) ist, hinzutreten. Für den ersten Fall gehört der Character Ω; 1 u. 3, 8 offenbar zu P und daher Ω; 5 u. 7, 8 zu Q, weshalb ihm ein negatives eigentlich primitives Geschlecht entspricht; und aus ähnlichem Grunde wird es im zweiten Falle ein Geschlecht in einer negativen eigentlich primitiven Ordnung geben, dessen Formen die vorgeschriebene Eigenschaft besitzen, dessen Character nämlich Ω; 3 u. 5, 8 ist.

Hieraus folgt, dass es negative primitive Formen mit der Determinante $-M$, deren characteristische Zahl 1 ist, giebt, wenn M irgend einer der Zahlen 1, 2, 3, 5, 6 nach dem Modul 8 congruent ist, und zwar stets in einem einzigen Geschlechte, welches ein uneigentliches im Falle $M \equiv 3$ ist, und dass es solche Formen überhaupt nicht giebt, wenn $M \equiv 0$, 4 oder 7 (mod. 8) ist. Übrigens ist klar, dass, wenn $(-a, -b, -c)$ eine negative primitive Form ist, deren characteristische Zahl $+1$ ist, (a, b, c) eine positive primitive Form mit der characteristischen Zahl -1 ist. Hieraus ist ersichtlich, dass es in den fünf ersten Fällen (wenn $M \equiv 1, 2, 3, 5, 6$ ist) ein positives primitives Geschlecht giebt, dessen Formen die characteristische Zahl -1 haben, und zwar für $M \equiv 3$ ein uneigentliches, dass es aber in den drei übrigen Fällen (wenn $M \equiv 0, 4, 7$ ist) derartige positive Formen überhaupt nicht geben kann.

289.

In Betreff der eigentlichen Darstellungen der binären Formen durch die ternäre Form $x^2+y^2+z^2=f$ ergiebt sich aus der im Artikel 282 angegebenen allgemeinen Theorie das Folgende:

I. Die binäre Form φ kann durch f nur eigentlich dargestellt werden, wenn es eine positive primitive Form und -1 (d. i. die Determinante der Form f) ihre characteristische Zahl ist. Daher giebt es für eine positive Determinante, sowie für eine negative $-M$, falls M entweder durch 4 teilbar oder von der Form $8n+7$ ist, keine durch f eigentlich darstellbaren binären Formen.

II. Ist aber $\varphi = (p, q, r)$ eine positive primitive Form mit der Determinante $-M$ und -1 die characteristische Zahl der Form φ und daher

auch der zu ihr entgegengesetzten $(p, -q, r)$, so giebt es zu jedem beliebigen gegebenen Werte des Ausdrucks $\sqrt{-(p, -q, r)}$ gehörige eigentliche Darstellungen der Form φ durch f. Es werden nämlich sämtliche Coefficienten der ternären Form g mit der Determinante -1 (Artikel 283) notwendig ganze Zahlen, g aber eine definitive Form und daher sicher f äquivalent (Artikel 285, I).

III. Die Anzahl aller zu demselben Werte des Ausdrucks $\sqrt{-(p, -q, r)}$ gehörigen Darstellungen ist in allen Fällen, ausser wenn $M = 1$ und $M = 2$ ist, nach Artikel 283, III ebenso gross, wie die Anzahl der Transformationen der Form f in g und daher nach Artikel 285 gleich 48; ebendaraus geht hervor, dass, wenn man eine zu einem gegebenen Werte gehörige Darstellung hat, die 47 andern daraus abgeleitet werden, indem man die Werte von x, y, z auf alle möglichen Weisen unter einander vertauscht und mit entgegengesetzten Zeichen nimmt; daher bringen sämtliche 48 Darstellungen nur eine einzige Zerlegung der Form φ in drei Quadrate hervor, wenn man nur auf die Quadrate selbst und nicht auf ihre Reihenfolge und die Vorzeichen ihrer Wurzeln Rücksicht nimmt.

IV. Setzt man die Anzahl aller in M aufgehenden von einander verschiedenen ungeraden Primzahlen gleich μ, so folgert man aus Artikel 233 ohne Schwierigkeit, dass die Anzahl aller verschiedenen Werte des Ausdrucks $\sqrt{-(p, -q, r)}$ (mod. M) gleich 2^{μ} ist, von denen man jedoch nach Artikel 283 nur die Hälfte zu betrachten hat (wenn $M > 2$ ist). Daher ist die Anzahl aller eigentlichen Darstellungen der Form φ durch f gleich $48 \cdot 2^{\mu-1} = 3 \cdot 2^{\mu+3}$, die Anzahl der verschiedenen Zerlegungen in drei Quadrate aber gleich $2^{\mu-1}$.

Beispiel. Es sei $\varphi = 19t^2 + 6tu + 41u^2$ und daher $M = 770$. Hier hat man folgende vier Werte des Ausdrucks $\sqrt{-(19, -3, 4)}$ (mod. 770) zu betrachten (Artikel 283): (39, 237), (171, -27), (269, -83), (291, -127). Um die zum Werte (39, 237) gehörigen Darstellungen zu finden, leite man zuerst die ternäre Form $\begin{pmatrix} 19, & 41, & 2 \\ 3, & 6, & 3 \end{pmatrix} = g$ her, in welche, wie man nach den Regeln im Artikel 272, 275 findet, f übergeht durch die Substitution $\begin{Bmatrix} 1, & -6, & 0 \\ -3, & -2, & -1 \\ -3, & -1, & -1 \end{Bmatrix}$, woraus man folgende Darstellung der Form φ durch f erhält:

$$x = t - 6u, \quad y = -3t - 2u, \quad z = -3t - u;$$

die 47 übrigen zu demselben Werte gehörigen Darstellungen, welche durch Permutation dieser Werte und Umkehrung der Vorzeichen sich ergeben, schreiben wir der Kürze wegen nicht hin. Sämtliche 48 Darstellungen aber bringen dieselbe Zelegung der Form φ in drei Quadrate

$$t^2 - 12tu + 36u^2, \quad 9t^2 + 12tu + 4u^2, \quad 9t^2 + 6tu + u^2$$

hervor.

Auf ganz ähnliche Weise ergiebt der Wert (171, — 27) die Zerlegung in die Quadrate $(3t+5u)^2$, $(3t-4u)^2$, t^2; der Wert (269, — 83) die folgende Zerlegung: $(t+6u)^2+(3t+u)^2+(3t-2u)^2$; schliesslich der Wert (291, — 127) die folgende: $(t+3u)^2+(3t+4u)^2+(3t-4u)^2$; diese einzelnen Zerlegungen sind den 48 Darstellungen äquivalent. — Ausser diesen 192 Darstellungen oder vier Zerlegungen aber giebt es keine weiter, da 770 durch kein Quadrat teilbar ist und somit uneigentliche Darstellungen nicht existieren können.

290.

Die Formen mit der Determinante — 1 und — 2, welche einigen Ausnahmen unterliegen, wollen wir kurz gesondert betrachten. Wir schicken die allgemeine Bemerkung voraus, dass, wenn φ, φ' irgend welche äquivalente binäre Formen sind und (θ) eine gegebene Transformation jener in diese ist, aus der Combination jeder Darstellung der Form φ durch irgend eine ternäre Form f mit der Substitution (θ) eine Darstellung der Form φ' durch f entspringt, ferner dass auf diese Weise aus eigentlichen Darstellungen von φ eigentliche Darstellungen der Form φ' und zwar aus verschiedenen verschiedene, aus allen sämtliche derartigen Darstellungen von φ' entstehen. Dies lässt sich durch die Rechnung sehr leicht nachweisen. Daher kann die eine der Formen φ, φ' auf ebenso viele Arten durch f dargestellt werden, wie die andere.

I. Es sei zunächst $\varphi = t^2+u^2$ und φ' irgend eine andere positive binäre Form mit der Determinante — 1, welcher die Form φ äquivalent ist, und es gehe φ in φ' über durch die Substitution $t=\alpha t'+\beta u'$, $u=\gamma t'+\delta u'$. Die Form φ wird dargestellt durch die ternäre Form $f=x^2+y^2+z^2$, wenn man setzt $x=t$, $y=u$, $z=0$; durch Vertauschung von x, y, z gehen hieraus sechs Darstellungen hervor, und aus jeder einzelnen wiederum vier, wenn man die Vorzeichen von t, u ändert, so dass man überhaupt 24 Darstellungen hat, denen eine einzige Zerlegung in drei Quadrate entspricht, und ausser denen es, wie man leicht sieht, keine andern weiter geben kann. Hieraus folgt, dass auch die Form φ' nur auf eine einzige Weise in drei Quadrate zerlegt werden kann, nämlich in $(\alpha t'+\beta u')^2$, $(\gamma t'+\delta u')^2$ und 0, welche Zerlegung 24 Darstellungen äquivalent ist.

II. Es sei $\varphi = t^2+2u^2$, φ' irgend eine andere positive binäre Form mit der Determinante — 2, und es gehe φ in diese über durch die Substitution $t=\alpha t'+\beta u'$, $u=\gamma t'+\delta u'$. Dann schliesst man in ähnlicher Weise wie im vorigen Falle, dass φ und somit auch φ' nur auf eine einzige Weise in drei Quadrate zerlegt werden kann, nämlich φ in $t^2+u^2+u^2$ und φ' in $(\alpha t'+\beta u')^2+(\gamma t'+\delta u')^2+(\gamma t'+\delta u')^2$; dass eine solche Zerlegung 24 Darstellungen äquivalent ist, ist leicht ersichtlich.

Hieraus folgt, dass die binären Formen mit den Determinanten — 1 und — 2 hinsichtlich der Anzahl der Darstellungen durch die ternäre Form $x^2+y^2+z^2$ mit den andern binären Formen vollständig übereinstimmen;

denn da in beiden Fällen $\mu = 0$ wird, so giebt die im vorigen Artikel angegebene Formel jedenfalls 24 Darstellungen. Der Grund hierfür ist, dass sich die beiden Ausnahmen, welchen solche Formen unterliegen, gegenseitig compensieren.

Wir entheben uns der Kürze wegen der Mühe, die im Artikel 284 dargestellte allgemeine Theorie der uneigentlichen Darstellungen auf die Form $x^2 + y^2 + z^2$ anzuwenden.

291.

Die Aufgabe, alle eigentlichen Darstellungen einer gegebenen positiven Zahl M durch die Form $x^2 + y^2 + z^2$ zu finden, wird nach Artikel 281 zunächst auf die Ermittlung der eigentlichen Darstellungen der Zahl $-M$ durch die Form $-x^2 - y^2 - z^2 = f$ zurückgeführt; diese aber leitet man nach den Vorschriften des Artikels 280 folgendermassen her:

I. Man entwickle sämtliche Klassen der binären Formen mit der Determinante $-M$, deren Formen durch $X^2 + Y^2 + Z^2 = F$ (welcher ternären Form die Form f adjungiert ist) eigentlich dargestellt werden können. Ist $M \equiv 0, 4, 7 \pmod{8}$, so giebt es nach Artikel 288 solche Klassen nicht, und daher lässt sich M nicht in drei Quadrate, welche keinen gemeinschaftlichen Teiler haben, zerlegen*). Ist aber $M \equiv 1, 2, 5$ oder 6, so giebt es ein positives eigentlich primitives und, wenn $M \equiv 3$ ist, ein uneigentlich primitives Geschlecht, welches alle jene Klassen umfasst; die Anzahl dieser Klassen bezeichnen wir mit k.

II. Man wähle nun aus diesen Klassen k Formen nach Belieben, aus jeder eine, aus, welche $\varphi, \varphi', \varphi'', \ldots$ sein mögen, ermittle sämtliche eigentlichen Darstellungen aller durch F, deren Anzahl somit gleich $3 \cdot 2^{\mu+3} k = K$ ist, wo μ die Anzahl der (ungeraden) Primfactoren von M bezeichnet, und leite endlich aus jeder derartigen Darstellung wie

$$X = mt + nu, \qquad Y = m't + n'u, \qquad Z = m''t + n''u$$

die folgende Darstellung von M durch $x^2 + y^2 + z^2$ her:

$$x = m'n'' - m''n', \quad y = m''n - mn'', \quad z = mn' - m'n.$$

In dem Complex dieser K Darstellungen, welchen wir mit Ω bezeichnen, sind notwendig sämtliche Darstellungen von M enthalten.

III. Wir haben daher nur noch zu untersuchen, ob in Ω identische Darstellungen vorkommen können; und da wir aus Artikel 280, III bereits wissen, dass diejenigen Darstellungen in Ω, welche aus verschiedenen Formen, z. B. aus φ und φ', abgeleitet sind, notwendig verschieden sind, so

*) Dies geht auch daraus hervor, dass die Summe dreier ungerader Quadrate notwendig $\equiv 3 \pmod{8}$ ist, die Summe zweier ungeraden und eines geraden entweder $\equiv 2$ oder $\equiv 6$, die Summe eines ungeraden und zweier geraden entweder $\equiv 1$ oder $\equiv 0$, endlich die Summe dreier geraden entweder $\equiv 0$ oder $\equiv 4$; im letzten Falle aber ist die Darstellung offenbar eine uneigentliche.

bleibt nur die Untersuchung übrig, ob verschiedene Darstellungen derselben Form, z, B. der Form φ, durch F identische Darstellungen der Zahl M durch $x^2+y^2+z^2$ hervorbringen können. Nun ist sogleich klar, dass, wenn sich unter den Darstellungen von φ die folgende befindet:

$$(r)\quad X=mt+nu,\qquad Y=m't+n'u,\qquad Z=m''t+n''u,$$

darunter auch die folgende vorkommt:

$$(r')\quad X=-mt-nu,\ Y=-m't-n'u,\ Z=-m''t-n''u,$$

und dass sich aus jeder der beiden dieselbe Darstellung der Zahl M ergiebt, welche mit (R) bezeichnet werden möge; wir untersuchen daher, ob sich dieselbe Darstellung (R) auch noch aus andern Darstellungen der Form φ ergeben kann. Aus Artikel 280, III folgt leicht, indem man daselbst $\chi=\varphi$ setzt, dass, wenn sämtliche eigentlichen Transformationen der Form φ in sich selbst durch

$$t=\alpha t+\beta u,\quad u=\gamma t+\delta u$$

dargestellt werden, sich alle diejenigen Darstellungen der Form φ, aus denen R folgt, ausdrücken durch:

$$\begin{aligned}x&=(\alpha m+\gamma n)t+(\beta m+\delta n)u\\ y&=(\alpha m'+\gamma n')t+(\beta m'+\delta n')u\\ z&=(\alpha m''+\gamma n'')t+(\beta m''+\delta n'')u.\end{aligned}$$

Aber aus der im Artikel 179 dargelegten Theorie der Transformation binärer Formen mit negativer Determinante ergiebt sich, dass es in allen Fällen, ausser wenn $M=1$ und $M=3$ ist, nur zwei eigentliche Transformationen der Form φ in sich selbst giebt, nämlich $\alpha, \beta, \gamma, \delta = 1, 0, 0, 1$ und $= -1, 0, 0, -1$ respective (da nämlich φ eine primitive Form ist, so ist das, was im Artikel 179 mit m bezeichnet wurde, entweder 1 oder 2 und somit wird, ausser in den ausgeschlossenen Fällen, sicher (1) hier stattfinden), Daher kann (R) nur aus (r), (r') hervorgehen und somit findet sich jede eigentliche Darstellung der Zahl M zweimal und nicht öfter in Ω vor, und die Anzahl aller verschiedenen eigentlichen Darstellungen von M ist gleich $\frac{1}{2}K=3\cdot 2^{\mu+2}k$.

Was die ausgenommenen Fälle angeht, so ist die Anzahl der eigentlichen Transformationen der Form φ in sich selbst nach Artikel 179 gleich 4 für $M=1$ und gleich 6 für $M=3$, und in der That bestätigt man leicht, dass die Anzahl der eigentlichen Darstellungen der Zahlen 1, 3 gleich $\frac{1}{4}K$, $\frac{1}{6}K$ respective ist; es kann nämlich jede der beiden Zahlen nur auf eine einzige Weise in drei Quadrate zerlegt werden, 1 in $1+0+0$, 3 in $1+1+1$; die Zerlegung von 1 liefert sechs, die Zerlegung von 3 acht verschiedene Darstellungen; K aber wird gleich 24 für $M=1$ (wo $\mu=0$, $k=1$ ist) und gleich 48 für $M=3$ (wo $\mu=1$, $k=1$ ist).

Übrigens bemerken wir, dass, wenn h die Anzahl der Klassen im Hauptgeschlechte ist, welcher nach Artikel 252 die Anzahl der Klassen in

jedem andern eigentlich primitiven Geschlechte gleich ist, $k = h$ für $M \equiv 1, 2, 5$ oder $6 \pmod{8}$, aber $k = \frac{1}{3}h$ für $M \equiv 3 \pmod{8}$ wird, den einen Fall $M = 3$ ausgenommen, in welchem $k = h = 1$ ist. Für die Zahlen von der Form $8n + 3$ ist daher allgemein die Anzahl der Darstellungen gleich $2^{\mu+2}h$, da sich bei der Zahl 3 zwei Ausnahmen compensieren.

292.

Die Zerlegungen der Zahlen (wie oben der binären Formen) in drei Quadrate unterscheiden wir von den Darstellungen durch die Form $x^2 + y^2 + z^2$ in der Weise, dass wir bei jenen nur auf die Grösse der Quadrate, bei diesen aber überdies auf die Reihenfolge derselben und die Vorzeichen ihrer Wurzeln Rücksicht nehmen und daher die Darstellungen $x = a$, $y = b$, $z = c$ und $x = a'$, $y = b'$, $z = c'$ für verschieden halten, wenn nicht gleichzeitig $a = a'$, $b = b'$, $c = c'$ ist, während wir die Zerlegungen in $a^2 + b^2 + c^2$ und $a'^2 + b'^2 + c'^2$ für eine einzige ansehen, wenn diese Quadrate ohne Rücksicht auf die Reihenfolge jenen gleich sind. Hieraus geht hervor:

I. dass die Zerlegung der Zahl M in die Quadrate $a^2 + b^2 + c^2$ 48 Darstellungen äquivalent ist, wenn keins von ihnen gleich 0 ist und alle ungleich sind, aber nur 24, wenn entweder eins gleich 0, die übrigen ungleich oder keins gleich 0 und zwei von ihnen einander gleich sind. Wenn aber in der Zerlegung einer gegebenen Zahl in drei Quadrate zwei von diesen gleich 0 sind oder eins gleich 0, die übrigen gleich, oder alle drei gleich sind, so wird dieselbe 6 oder 12 oder 8 Darstellungen äquivalent sein; doch kann dies nur in den besonderen Fällen, wo $M = 1$ oder 2 oder 3 respective ist, eintreten, wofern nämlich die Darstellungen eigentliche sein sollen. Wir schliessen diese aus und nehmen an, die Anzahl aller Zerlegungen der Zahl M in drei Quadrate (ohne gemeinschaftlichen Teiler) sei gleich E, und unter diesen befänden sich e, in denen ein Quadrat gleich 0, und e', in denen zwei Quadrate gleich sind; jene können auch als Zerlegungen in zwei Quadrate, diese als Zerlegungen in ein Quadrat und das Doppelte eines Quadrats betrachtet werden. Alsdann ist die Anzahl aller eigentlichen Darstellungen der Zahl M durch $x^2 + y^2 + z^2$ gleich

$$24(e + e') + 48(E - e - e') = 48E - 24(e + e').$$

Aus der Theorie der binären Formen folgt aber leicht, dass e entweder gleich 0 oder gleich $2^{\mu-1}$ ist, je nachdem -1 quadratischer Nichtrest oder Rest von M ist, und ebenso e' gleich 0 oder gleich $2^{\mu-1}$, je nachdem -2 Nichtrest oder Rest von M ist, wo μ die Anzahl der (ungeraden) Primfactoren von M ist (vgl. Artikel 182; eine ausführlichere Auseinandersetzung unterdrücken wir hier). Hieraus folgert man leicht, dass

$E = 2^{\mu-2}k$, wenn sowohl -1 als auch -2 Nichtreste von M sind,
$E = 2^{\mu-2}(k + 2)$, wenn beide Zahlen Reste sind,
$E = 2^{\mu-2}(k + 1)$, wenn die eine Zahl Rest, die andere Nichtrest von M ist.

In den ausgeschlossenen Fällen $M=1$ und $M=2$ würde diese Formel $E=\frac{3}{4}$ ergeben, während $E=1$ sein muss; für $M=3$ ergiebt sich aber richtig $E=1$, indem sich die Ausnahmen gegenseitig compensieren.

Ist daher M eine Primzahl, so wird $\mu=1$ und daher $E=\frac{1}{2}(k+2)$, falls $M\equiv 1 \pmod{8}$ und $E=\frac{1}{2}(k+1)$, falls $M\equiv 3$ oder $\equiv 5$ ist. Diese speciellen Sätze sind von Legendre auf inductivem Wege entdeckt und in der ausgezeichneten schon öfter angeführten Abhandlung *Hist. de l'Ac. de Paris 1785 p. 530 u. ff.* veröffentlicht worden, wenn auch in einer etwas verschiedenen Form, wofür der Grund hauptsächlich darin liegt, dass er die eigentliche Äquivalenz nicht von der uneigentlichen unterschied und daher entgegengesetzte Klassen mit einander vermischte.

II. Um sämtliche Zerlegungen einer Zahl M in drei Quadrate (ohne gemeinschaftlichen Teiler) zu finden, braucht man nicht sämtliche eigentlichen Darstellungen aller Formen $\varphi, \varphi', \varphi'', \ldots$ zu ermitteln. Denn zunächst bestätigt man leicht, dass sämtliche 48 Darstellungen der Form φ, welche zu demselben Werte des Ausdrucks $\sqrt{-(p, -q, r)}$ (wenn $\varphi = (p, q, r)$ gesetzt wird) gehören, ein und dieselbe Zerlegung der Zahl M liefern, und es daher genügt, wenn man nur eine von ihnen hat, oder, was auf dasselbe hinauskommt, wenn nur alle verschiedenen Zerlegungen*) der Form φ in drei Quadrate gefunden sind, und ebenso bei den übrigen $\varphi', \varphi'', \ldots$ Ferner kann man, wenn φ aus einer nicht ambigen Klasse ist, diejenige Form, welche aus der entgegengesetzten Klasse ausgewählt ist, ganz übergehen, oder es genügt, von je zwei entgegengesetzten Klassen nur eine einzige zu betrachten. Denn da es vollständig gleichgültig ist, welche Form aus den einzelnen Klassen ausgewählt wird, so wollen wir annehmen, dass aus der Klasse, welche derjenigen, zu welcher φ gehört, entgegengesetzt ist, die zu φ entgegengesetzte Form, welche gleich φ' sei, ausgewählt worden sei. Dann sieht man leicht, dass, wenn die eigentlichen Zerlegungen der Form φ unbestimmt durch

$$(gt+hu)^2+(g't+h'u)^2+(g''t+h''u)^2$$

dargestellt werden, alle Zerlegungen von φ' ausgedrückt werden durch

$$(gt-hu)^2+(g't-h'u)^2+(g''t-h''u)^2,$$

sowie dass aus diesen eben dieselben Darstellungen der Zahl M sich ergeben wie aus jenen. Endlich kann man in dem Falle, wo φ eine Form aus einer ambigen Klasse, jedoch weder aus der Hauptklasse ist, noch der Form $(2, 0, \frac{1}{2}M)$ oder der Form $(2, 1, \frac{1}{2}(M+1))$ (je nachdem M gerade oder ungerade ist) äquivalent ist, von den Werten des Ausdrucks $\sqrt{-(p, -q, r)}$ die Hälfte weglassen; der Kürze wegen setzen wir aber diesen Vorteil nicht ausführlicher auseinander. — Übrigens können wir uns desselben

*) Man muss immer „eigentliche“ hinzudenken, wenn man diesen Ausdruck von den Darstellungen auf die Zerlegungen übertragen will.

Vorteils bedienen, wenn wir sämtliche eigentlichen Darstellungen der Zahl M durch $x^2+y^2+z^2$ haben wollen, da diese sich aus den Zerlegungen leicht ergeben.

Beispiels halber wollen wir sämtliche Zerlegungen der Zahl 770 in drei Quadrate suchen. Hierbei ist $\mu=3$, $e=e'=0$ und daher $E=2k$. Gemäss der Klassifikation der positiven binären Formen mit der Determinante -770, die wir hier, weil sie von jedem nach der Vorschrift des Artikels 231 leicht aufgestellt werden kann, der Kürze wegen nicht herschreiben, findet man die Anzahl der positiven Klassen gleich 32, welche sämtlich eigentlich primitiv sind und in 8 Geschlechter zerfallen, so dass $k=4$ und somit $E=8$ ist. Das Geschlecht, dessen characteristische Zahl -1 ist, muss in Bezug auf die Zahlen 5, 7, 11 offenbar die Specialcharactere $R5$; $N7$; $N11$ haben, woraus nach Artikel 263 leicht folgt, dass sein Character in Bezug auf die Zahl 8 der folgende: 1 u. 3, 8 sein muss. Nun finden sich in dem Geschlechte, dessen Character 1 u. 3, 8; $R5$; $N7$; $N11$ ist, vier Klassen, als deren Repräsentanten wir die Formen auswählen: (6, 2, 129), (6, -2, 129), (19, 3, 41), (19, -3, 41); die zweite und vierte Klasse lassen wir aber weg, da sie der ersten und dritten respective entgegengesetzt sind. Die vier Zerlegungen der Form (19, 3, 41) haben wir schon im Artikel 289 angegeben; aus ihnen ergeben sich die Zerlegungen der Zahl 770 in $9+361+400$, $16+25+729$, $81+400+289$, $576+169+25$. Auf ähnliche Weise findet man die vier Zerlegungen der Form $6t^2+4tu+129u^2$ in

$$(t-8u)^2+(2t+u)^2+(t+8u)^2,\quad (t-10u)^2+(2t+5u)^2+(t+2u)^2$$
$$(2t-5u)^2+(t+10u)^2+(t+2u)^2,\quad (2t+7u)^2+(t-8u)^2+(t-4u)^2,$$

welche bezüglich aus den folgenden Werten des Ausdrucks $\sqrt{-(6, -2, 129)}$ sich ergeben: (48, 369), (62, -149), (92, -159), (202, 61). Hieraus gehen die Zerlegungen der Zahl 770 in $225+256+289$, $1+144+625$, $64+81+625$, $16+225+529$ hervor. Ausser diesen acht Zerlegungen giebt es keine weiter.

Was sich auf die Zerlegungen der Zahlen in drei Quadrate, welche einen gemeinschaftlichen Teiler haben, bezieht, ergiebt sich aus der allgemeinen Theorie des Artikels 281 so leicht, dass wir uns damit nicht aufzuhalten brauchen.

Beweis der Fermat'schen Sätze, dass jede ganze Zahl in drei Trigonalzahlen oder in vier Quadrate zerlegt werden kann.

293.

Die vorstehenden Untersuchungen liefern auch einen Beweis des berühmten **Satzes**, dass jede positive ganze Zahl in drei Trigonal-

zahlen zerlegt werden kann, ein Satz, der von Fermat einst gefunden worden ist, für den es aber bisher an einem strengen Beweise fehlte. Offenbar giebt jede Zerlegung der Zahl M in Trigonalzahlen

$$\tfrac{1}{2}x(x+1)+\tfrac{1}{2}y(y+1)+\tfrac{1}{2}z(z+1)$$

Veranlassung zu einer Zerlegung der Zahl $8M+3$ in drei ungerade Quadrate

$$(2x+1)^2+(2y+1)^2+(2z+1)^2$$

und umgekehrt. Nach der vorstehenden Theorie ist aber jede ganze positive Zahl $8M+3$ in drei Quadrate zerlegbar, welche notwendig ungerade sind (Vgl. die Anmerkung zu Artikel 291), und die Anzahl der Zerlegungen hängt ab sowohl von der Anzahl der Primfactoren von $8M+3$ als auch von der Anzahl der Klassen, in welche die binären Formen mit der Determinante $-(8M+3)$ zerfallen. Ebensoviele Zerlegungen der Zahl M in drei Trigonalzahlen giebt es. Wir setzen dabei aber voraus, dass $\frac{1}{2}x(x+1)$ für jeden beliebigen Wert von x als Trigonalzahl betrachtet werde; will man aber lieber die Null ausschliessen, so müsste man den Satz so abändern: Jede ganze positive Zahl ist entweder selbst eine Trigonalzahl oder in zwei oder in drei Trigonalzahlen zerlegbar. Eine ähnliche Änderung müsste man in dem folgenden Satze eintreten lassen, wenn man die Null von den Quadraten ausschliessen wollte.

Nach denselben Prinzipien wird ein anderer Fermat'scher Satz bewiesen, nämlich dass jede ganze positive Zahl in vier Quadrate zerlegt werden kann. Subtrahiert man von einer Zahl von der Form $4n+2$ ein beliebiges Quadrat (welches kleiner ist als jene Zahl), von einer Zahl von der Form $4n+1$ ein gerades oder von einer Zahl von der Form $4n+3$ ein ungerades Quadrat, so ist der Rest in allen diesen Fällen in drei Quadrate zerlegbar, und daher die gegebene Zahl in vier. Endlich kann eine Zahl von der Form $4n$ dargestellt werden durch $4^\mu N$, so dass N zu irgend einer der vorigen drei Formen gehört; ist aber N in vier Quadrate zerlegt, so wird auch $4^\mu N$ in dieser Weise zerlegt sein. Von einer Zahl von der Form $8n+3$ kann auch ein Quadrat mit gerademal gerader Wurzel, von einer Zahl von der Form $8n+7$ ein Quadrat mit ungerademal gerader Wurzel, von einer Zahl von der Form $8n+4$ ein ungerades Quadrat abgezogen werden, und der Rest wird immer in drei Quadrate zerlegbar sein. Übrigens ist dieser Satz schon von Lagrange bewiesen worden, *Nouv. Mém. de l'Ac. de Berlin 1770, p. 123,* und diesen Beweis (der von dem unsrigen völlig verschieden ist) hat Euler ausführlicher dargelegt in den *Actis Ac. Petr. Vol. II p. 48.* — Die andern Sätze Fermat's, welche gleichsam die Fortsetzung der vorstehenden bilden, nämlich dass jede ganze Zahl in fünf Pentagonalzahlen, sechs Hexagonalzahlen, sieben Heptagonalzahlen u. s. w. zerlegbar sei, entbehren bisher noch des Beweises und scheinen andere Prinzipien zu erfordern.

Auflösung der Gleichung $ax^2 + by^2 + cz^2 = 0$.

294.

Satz. Bezeichnen a, b, c zu einander prime Zahlen, von denen keine gleich 0 noch durch ein Quadrat teilbar ist, so besitzt die Gleichung

$$(\Omega) \qquad ax^2 + by^2 + cz^2 = 0$$

(ausser $x = y = z = 0$, die wir unberücksichtigt lassen) keine Lösung in ganzen Zahlen, wenn nicht $-bc$, $-ac$, $-ab$ respective quadratische Reste von a, b, c sind und diese Zahlen ungleiche Vorzeichen besitzen; sind aber diese vier Bedingungen erfüllt, so ist die Gleichung (Ω) in ganzen Zahlen auflösbar.

Beweis. Wenn (Ω) überhaupt durch ganze Zahlen lösbar ist, so wird sie auch durch solche Werte von x, y, z gelöst werden können, welche keinen gemeinschaftlichen Teiler haben; denn irgendwelche der Gleichung (Ω) genügende Werte werden ihr auch genügen, wenn sie durch den grössten gemeinschaftlichen Teiler dividiert werden. Nimmt man nun an, dass $ap^2 + bq^2 + cr^2 = 0$ und p, q, r von einem gemeinschaftlichen Teiler frei seien, so werden sie auch unter einander prim sein; denn wenn q, r einen gemeinschaftlichen Teiler μ hätten, so würde dieser zu p prim sein, μ^2 aber würde in ap^2 und somit in a aufgehen, was der Voraussetzung widerspricht; und ebenso sind p, r; p, q prim zu einander. Es wird daher $-ap^2$ durch die binäre Form $by^2 + cz^2$ dargestellt, wenn man y, z die zu einander primen Werte q, r beilegt, weshalb die Determinante $-bc$ derselben quadratischer Rest von ap^2 und daher auch von a ist (Artikel 154). In derselben Weise ist $-acRb$, $-abRc$. Dass aber (Ω) keine Lösung haben kann, wenn a, b, c dasselbe Vorzeichen besitzen, ist so klar, dass es einer Auseinandersetzung nicht bedarf.

Den Beweis des umgekehrten Satzes, welcher den zweiten Teil unseres Theorems bildet, führen wir so, dass wir zunächst zeigen, wie man eine ternäre der Form $\begin{pmatrix} a, & b, & c \\ 0, & 0, & 0 \end{pmatrix} = f$ äquivalente Form finden kann, deren zweiter, dritter, vierter Coefficient durch a, b, c teilbar ist, und daraus dann zweitens die Lösung der Gleichung (Ω) ableiten.

I. Man suche drei Zahlen A, B, C, welche keinen gemeinschaftlichen Teiler haben und so beschaffen sind, dass A prim zu b und c, B prim zu a und c, C prim zu a und b ist, $aA^2 + bB^2 + cC^2$ aber durch abc teilbar ist. Dies geschieht auf folgende Weise. Es seien $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ respective Werte der Ausdrücke $\sqrt{-bc}$ (mod. a), $\sqrt{-ac}$ (mod. b), $\sqrt{-ab}$ (mod. c), welche notwendig zu a, b, c respective prim sind. Man nehme drei ganze Zahlen $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ völlig nach Belieben nur so an, dass sie respective zu a, b, c prim (z. B. alle gleich 1) sind, und bestimme A, B, C so, dass

$$A \equiv \mathfrak{b}c (\text{mod. } b) \text{ und } \equiv \mathfrak{c}\mathfrak{C} (\text{mod. } c)$$
$$B \equiv \mathfrak{c}a (\text{mod. } c) \text{ und } \equiv \mathfrak{a}\mathfrak{A} (\text{mod. } a)$$
$$C \equiv \mathfrak{a}b (\text{mod. } a) \text{ und } \equiv \mathfrak{b}\mathfrak{B} (\text{mod. } b)$$

wird. Dann ist:

$$aA^2 + bB^2 + cC^2 \equiv \mathfrak{a}^2(b\mathfrak{A}^2 + cb^2) \equiv \mathfrak{a}^2(b\mathfrak{A}^2 - \mathfrak{A}^2 b) \equiv 0 \ (\text{mod. } a)$$

oder durch a teilbar und ebenso durch b, c und somit auch durch das Product abc. Ausserdem geht hervor, dass A notwendig zu b und c, B zu a und c, C zu a und b prim ist. Wenn aber diese Werte von A, B, C einen (grössten) gemeinschaftlichen Teiler μ haben, so wird dieser offenbar zu a, b, c und daher auch zu abc prim sein; daher werden wir, indem wir jene Werte durch μ dividieren, neue Werte erhalten, welche keinen gemeinschaftlichen Teiler haben, den Wert von $aA^2 + bB^2 + cC^2$ auch noch durch abc teilbar machen und daher allen Bedingungen genügen.

II. Sind die Zahlen A, B, C auf diese Weise bestimmt, so werden auch Aa, Bb, Cc keinen gemeinschaftlichen Teiler haben. Denn hätten sie einen gemeinschaftlichen Teiler μ, so müsste dieser notwendig zu a prim sein (da a sowohl zu Bb als zu Cc prim ist) und ebenso prim zu b und c; daher müsste μ auch in A, B, C aufgehen, was der Voraussetzung widerspricht. Man kann daher ganze Zahlen α, β, γ von der Beschaffenheit finden, dass $\alpha Aa + \beta Bb + \gamma Cc = 1$ ist; man suche ferner sechs ganze Zahlen α', β', γ', α'', β'', γ'' von solcher Art, dass

$$\beta'\gamma'' - \beta''\gamma' = Aa, \quad \gamma'\alpha'' - \alpha'\gamma'' = Bb, \quad \alpha'\beta'' - \beta'\alpha'' = Cc$$

ist. Geht nun f durch die Substitution

$$\begin{matrix} \alpha, & \alpha', & \alpha'' \\ \beta, & \beta', & \beta'' \\ \gamma, & \gamma', & \gamma'' \end{matrix}$$

in die Form $\begin{pmatrix} m, & m', & m'' \\ n, & n', & n'' \end{pmatrix} = g$ (welche f äquivalent sein wird) über, so behaupte ich, dass m', m'', n durch abc teilbar sind. Setzt man nämlich:

$$\beta''\gamma - \gamma''\beta = A', \quad \gamma''\alpha - \alpha''\gamma = B', \quad \alpha''\beta - \beta''\alpha = C',$$
$$\beta\gamma' - \gamma\beta' = A'', \quad \gamma\alpha' - \alpha\gamma' = B'', \quad \alpha\beta' - \beta\alpha' = C'',$$

so wird:

$$\alpha' = B''Cc - C''Bb, \quad \beta' = C''Aa - A''Cc, \quad \gamma' = A''Bb - B''Aa$$
$$\alpha'' = C'Bb - B'Cc, \quad \beta'' = A'Cc - C'Aa, \quad \gamma'' = B'Aa - A'Bb.$$

Werden diese Werte in die Gleichungen

$$m' = a\alpha'^2 + b\beta'^2 + c\gamma'^2$$
$$m'' = a\alpha''^2 + b\beta''^2 + c\gamma''^2$$
$$n = a\alpha'\alpha'' + b\beta'\beta'' + c\gamma'\gamma''$$

substituiert, so ergiebt sich nach dem Modul a:

$$\begin{aligned} m' &\equiv bcA''^2 \ (B^2b + C^2c) \equiv 0 \\ m'' &\equiv bcA'^2 \ (B^2b + C^2c) \equiv 0 \\ n &\equiv bcA'A'' (B^2b + C^2c) \equiv 0, \end{aligned}$$

d. h. m', m'', n sind durch a teilbar; und auf analoge Weise findet man, dass dieselben Zahlen durch b, c und somit auch durch abc teilbar sind.

III. Setzen wir der Kürze wegen die Determinante der Formen f, g d. h. die Zahl $-abc = d$,

$$md = M, \quad m' = M'd, \quad m'' = M''d, \quad n = Nd, \quad n' = N', \quad n'' = N'',$$

so geht offenbar f durch die Substitution (S)

$$\begin{matrix} \alpha d, & \alpha', & \alpha'' \\ \beta d, & \beta', & \beta'' \\ \gamma d, & \gamma', & \gamma'' \end{matrix}$$

in die ternäre Form $\begin{pmatrix} Md, & M'd, & M''d \\ Nd, & N'd, & N''d \end{pmatrix} = g'$ mit der Determinante d^3 über, welche somit unter f enthalten ist. Ich behaupte nun, dass dieser Form g' notwendig die Form $\begin{pmatrix} d, & 0, & 0 \\ d, & 0, & 0 \end{pmatrix} = g''$ äquivalent ist. Denn offenbar ist $\begin{pmatrix} M, & M', & M'' \\ N, & N', & N'' \end{pmatrix} = g'''$ eine ternäre Form mit der Determinante 1; ferner ist, da nach Voraussetzung a, b, c nicht dasselbe Vorzeichen haben, f eine indefinite Form, woraus leicht folgt, dass auch g' und g''' indefinit sein müssen; somit ist g''' der Form $\begin{pmatrix} 1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$ äquivalent (Artikel 277), und es lässt sich eine Transformation (S') jener in diese finden; offenbar aber wird durch (S') die Form g' in g'' übergehen. Hiernach ist auch g'' unter f enthalten und durch Combination der Substitutionen (S), (S') ergiebt sich eine Transformation der Form f in g''. Ist diese

$$\begin{matrix} \delta,, & \delta', & \delta'' \\ \varepsilon, & \varepsilon', & \varepsilon'' \\ \zeta, & \zeta' & \zeta'', \end{matrix}$$

so ist klar, dass man eine doppelte Lösung der Gleichung (Ω) erhält, nämlich $x = \delta'$, $y = \varepsilon'$, $z = \zeta'$ und $x = \delta''$, $y = \varepsilon''$, $z = \zeta''$; zugleich geht daraus hervor, dass keines der beiden Wertsysteme gleich Null sein kann, da notwendig

$$\delta\varepsilon'\zeta'' + \delta'\varepsilon''\zeta + \delta''\varepsilon\zeta' - \delta\varepsilon''\zeta' - \delta'\varepsilon\zeta'' - \delta''\varepsilon'\zeta = d$$

ist.

Beispiel. Die gegebene Gleichung sei $7x^2 - 15y^2 + 23z^2 = 0$; dieselbe ist lösbar, weil $345R7$, $-161R15$, $105R23$ ist. Man erhält für $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$

die Werte 3, 7, 6 und setzt man $\mathfrak{a}=\mathfrak{b}=\mathfrak{c}=1$, so findet man $A=98$, $B=-39$, $C=-8$. Hieraus leitet man die Substitution $\begin{Bmatrix} 3, & 5, & 22 \\ -1, & 2, & -28 \\ 8, & 25, & -7 \end{Bmatrix}$ her, durch welche f übergeht in $\begin{pmatrix} 1520, & 14490, & -7245 \\ -2415, & -1246, & 4735 \end{pmatrix} = g$. Hieraus wird:

$$(S)=\begin{Bmatrix} 7245, & 5, & 22 \\ -2415, & 2, & -28 \\ 19320, & 25, & -7 \end{Bmatrix}, \quad g'''=\begin{pmatrix} 3670800, & 6, & -3 \\ -1, & -1246, & 4735 \end{pmatrix}.$$

Ferner findet man, dass die Form g''' in $\begin{pmatrix} 1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$ übergeht durch die Substitution:

$$(S')=\begin{Bmatrix} 3, & 5, & 1 \\ -2440, & -4066, & -813 \\ -433, & -722, & -144 \end{Bmatrix},$$

und wird diese mit (S) combiniert, so ergiebt sich folgende: $\begin{Bmatrix} 9, & 11, & 12 \\ -1, & 9, & -9 \\ -9, & 4, & 3 \end{Bmatrix}$, durch welche f in g'' übergeht. Wir erhalten daher die doppelte Lösung der gegebenen Gleichung: $x=11$, $y=9$, $z=4$ und $x=12$, $y=-9$, $z=3$. Die letztere wird einfacher, wenn man die Werte durch den gemeinschaftlichen Teiler 3 dividiert, also $x=4$, $y=-3$, $z=1$.

295.

Der letzte Teil des Satzes im vorigen Artikel kann auch auf folgende Weise erledigt werden. Man suche eine ganze Zahl h von der Beschaffenheit, dass $ah \equiv \mathfrak{C}$ (mod. c) ist (die Buchstaben $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ nehmen wir in derselben Bedeutung wie im vorigen Artikel), und es werde $ah^2+b=ci$ gesetzt. Dann sieht man leicht, dass i eine ganze Zahl und $-ab$ die Determinante der binären Form $(ac, ah, i)=\varphi$ ist. Diese Form ist sicher nicht positiv (denn da nach Voraussetzung a, b, c nicht dasselbe Zeichen haben, können ab und ac nicht gleichzeitig positiv sein); ferner hat sie die characteristische Zahl -1, was wir synthetisch folgendermassen beweisen: Bestimmt man ganze Zahlen e, e' derart, dass

$$e\equiv 0 \,(\text{mod. } a) \text{ und } \equiv \mathfrak{B} \,(\text{mod. } b), \quad ce'\equiv \mathfrak{A} \,(\text{mod. } a) \text{ und } \equiv h\mathfrak{B} \,(\text{mod. } b)$$

wird, so ist (e, e') der Wert des Ausdrucks $\sqrt{-(ac, ah, i)}$ (mod. $-ab$). Denn nach dem Modul a ist:

$$e^2\equiv 0 \equiv -ac, \qquad ee'\equiv 0 \equiv -ah$$
$$c^2e'^2\equiv \mathfrak{A}^2 \equiv -bc \equiv -c^2 i \text{ und daher } e'^2 \equiv -i;$$

nach dem Modul b aber ist:

$$e^2 \equiv \mathfrak{B}^2 \equiv -ac,\ cee' \equiv h\mathfrak{B}^2 \equiv -ach, \text{ und daher } ee' \equiv -ah$$
$$c^2e'^2 \equiv h^2\mathfrak{B}^2 \equiv -ach^2 \equiv -c^2i \text{ und daher } e'^2 \equiv -i.$$

Dieselben drei Congruenzen aber, welche nach jedem der beiden Moduln a, b stattfinden, gelten auch nach dem Modul ab. Hieraus folgt nach der Theorie der ternären Formen leicht, dass φ durch die Form $\begin{pmatrix} -1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$ darstellbar ist. Es sei also:

$$act^2 + 2ahtu + iu^2 = -(\alpha t + \beta u)^2 + 2(\gamma t + \delta u)(\varepsilon t + \zeta u),$$

dann ist, wenn man mit c multipliciert:

$$a(ct + hu)^2 + bu^2 = -c(\alpha t + \beta u)^2 + 2c(\gamma t + \delta u)(\varepsilon t + \zeta u).$$

Hieraus geht hervor, dass, wenn man t, u solche bestimmten Werte beilegt, dass entweder $\gamma t + \delta u$ oder $\varepsilon t + \zeta u = 0$ wird, man eine Lösung der Gleichung (Ω) erhält, der somit genügt werden wird sowohl durch

$$x = \delta c - \gamma h, \quad y = \gamma, \quad z = \alpha\delta - \beta\gamma,$$

als auch durch

$$x = \zeta c - \varepsilon h, \quad y = \varepsilon, \quad z = \alpha\zeta - \beta\varepsilon.$$

Zugleich ist klar, dass weder jene Werte noch diese gleichzeitig gleich 0 werden können; denn wenn $\delta c - \gamma h = 0$ und $\gamma = 0$ wäre, so würde auch $\delta = 0$ und $\varphi = -(\alpha t + \beta u)^2$, somit $ab = 0$ sein, was der Voraussetzung widerspricht, und ebenso bezüglich der andern Werte. — In unserm Beispiele finden wir für φ die folgende Form: $(161, -63, 24)$, den Wert des Ausdrucks $\sqrt{-\varphi}$ (mod. 105) $= (7, -51)$ und als Darstellung der Form φ durch $\begin{pmatrix} -1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$ die folgende:

$$\varphi = -(13t - 4u)^2 + 2(11t - 4u)(15t - 5u),$$

woraus sich die Lösungen ergeben: $x = 7, y = 11, z = -8$; $x = 20, y = 15, z = -5$, oder wenn man die letztere durch 5 dividiert und das Vorzeichen von z weglässt: $x = 4, y = 3, z = 1$.

Von diesen beiden Methoden, die Gleichung Ω zu lösen, besitzt die letztere den Vorzug, dass sie meistens mit kleineren Zahlen zu thun hat; die erstere aber, welche auch durch verschiedene hier zu übergehende Kunstgriffe zusammengezogen werden kann, erscheint besonders aus dem Grunde als die elegantere, weil sie die Zahlen a, b, c in genau derselben Weise behandelt und die Rechnung durch Vertauschung dieser in nichts geändert wird. Dies verhält sich im zweiten Falle anders, da in diesem die Rechnung meistenteils am bequemsten wird, wenn man für a die kleinste, für c die grösste der drei gegebenen Zahlen nimmt, wie wir es in unserm Beispiele gethan haben.

Über die Methode, nach welcher Legendre das Fundamentaltheorem behandelt hat.*)

296.

Das elegante, in den vorstehenden Artikeln entwickelte Theorem ist zuerst von Legendre *Hist. de l'Ac. de Paris 1785, p. 507,* gefunden und durch einen schönen (von den unsrigen beiden völlig verschiedenen) Beweis erhärtet worden. Zugleich aber versuchte dieser ausgezeichnete Geometer am angeführten Orte, einen Beweis für die Sätze, welche mit dem Fundamentaltheorem des vorigen Abschnittes übereinkommen, daraus abzuleiten, der, wie wir schon oben erklärt haben (Artikel 151), unserer Ansicht nach seinen Zweck nicht ganz erfüllt. Es ist daher hier der Ort, diesen (an sich höchst eleganten) Beweis kurz darzulegen und die Gründe für unsere Meinung anzugeben. Es wird folgende Bemerkung vorausgeschickt: Wenn die Zahlen a, b, c sämtlich $\equiv 1$ (mod. 4) sind, kann die Gleichung $ax^2 + by^2 + cz^2 = 0$ oder (Ω) nicht lösbar sein. Denn man sieht leicht, dass der Wert von $ax^2 + by^2 + cz^2$ in diesem Falle notwendig entweder $\equiv 1$ oder $\equiv 2$ oder $\equiv 3$ (mod. 4) wird, wenn nicht alle Grössen x, y, z gleichzeitig gerade angenommen werden. Wenn daher (Ω) lösbar wäre, so könnte dies nur durch gerade Werte von x, y, z geschehen, was absurd ist, da ja irgend welche der Gleichung (Ω) genügende Werte derselben auch noch genügen, wenn sie durch den grössten gemeinschaftlichen Teiler dividiert werden, wodurch notwendig mindestens einer eine ungerade Zahl wird. Nun werden die verschiedenen Fälle des zu beweisenden Satzes auf die folgenden Hauptpunkte zurückgeführt:

I. Bezeichnen p, q (positive ungleiche) Primzahlen von der Form $4n+3$, so kann nicht gleichzeitig pRq, qRp sein. Denn wenn dies möglich wäre, würden offenbar, wenn man $1 = a$, $-p = b$, $-q = c$ setzt, alle zur Lösbarkeit der Gleichung $ax^2 + by^2 + cz^2 = 0$ erforderlichen Bedingungen erfüllt sein (Artikel 294); dieselbe besitzt aber nach der vorausgeschickten Bemerkung keine Lösung; mithin kann die Annahme nicht richtig sein. Hieraus folgt sogleich der Satz 7 im Artikel 131.

II. Ist p eine Primzahl von der Form $4n+1$, q eine Primzahl von der Form $4n+3$, so kann nicht zugleich qRp, pNq sein. Denn sonst würde $-pRq$ und die Gleichung $x^2 + py^2 - qz^2 = 0$ lösbar sein, welche Gleichung jedoch nach der vorausgeschickten Bemerkung keine Auflösung besitzt. Hieraus ergeben sich die Fälle 4 und 5 im Artikel 131.

III. Sind p, q Primzahlen von der Form $4n+1$, so kann nicht zugleich pRq, qNp sein. Man nehme eine andere Primzahl r von der Form $4n+3$, welche Rest von q und von welcher p Nichtrest ist. Dann wird nach den

*) Vgl. die Zusätze am Schlusse der *Disquisitiones.*

eben (II) bewiesenen Fällen qRr, rNp. Wenn daher pRq, qNp wäre, würde $qrRp$, $prRq$, $pqNr$ und somit $-pqRr$ sein. Demnach würde im Widerspruch mit der vorausgeschickten Bemerkung die Gleichung $px^2+qy^2-rz^2=0$ lösbar sein; es kann daher die Annahme nicht bestehen. Hieraus ergeben sich die Fälle 1 und 2 des Artikels 131.

Kürzer behandelt man diesen Fall folgendermassen: Bezeichnet r eine Primzahl von der Form $4n+3$, von welcher p Nichtrest ist, so ist auch rNp und daher (wenn man pRq, qNp annimmt) $qrRp$; ferner $-pRq$, $-pRr$ und somit auch $-pRqr$; mithin würde die Gleichung $x^2+py^2-qrz^2=0$ lösbar sein, was der vorausgeschickten Bemerkung widerspricht. Hiernach u. s. w.

IV. Ist p eine Primzahl von der Form $4n+1$, q eine Primzahl von der Form $4n+3$, so kann nicht zugleich pRq, qNp sein. Man nehme eine Hülfsprimzahl r von der Form $4n+1$ an, welche Nichtrest jeder der beiden Zahlen p, q ist. Dann ist (nach II) qNr und (nach III) pNr; hieraus $pqRr$. Wenn daher pRq, qNp wäre, hätte man auch $prNq$, $-prRq$, $qrRp$; somit würde die Gleichung $px^2-qy^2+rz^2=0$ lösbar sein, was absurd ist. — Hieraus ergeben sich die Fälle 3 und 6 im Artikel 131.

V. Bezeichnen p, q Primzahlen von der Form $4n+3$, so kann nicht zugleich pNq, qNp sein. Denn setzt man voraus, dass dies möglich sei, und nimmt man eine Hülfsprimzahl r von der Form $4n+1$ an, welche Nichtrest einer jeden der beiden Zahlen p, q ist, so ist $qrRp$, $prRq$; ferner (nach II) pNr, qNr, somit $pqRr$ und $-pqRr$. Hiernach würde die Gleichung $-px^2-qy^2+rz^2=0$ möglich sein, was im Widerspruch steht mit der vorausgeschickten Bemerkung. Hieraus folgt der Fall 8 im Artikel 131.

297.

Betrachtet man den vorstehenden Beweis genauer, so wird man leicht erkennen, dass die Fälle I und II derart erledigt sind, dass sich nichts dagegen einwenden lässt. Die Beweise der übrigen Fälle stützen sich aber auf die Existenz von Hülfszahlen, und wenn diese noch nicht bewiesen ist, verliert die Methode offenbar alle Bedeutung. Obwohl diese Annahmen so beschaffen sind, dass es bei geringerer Aufmerksamkeit scheinen könnte, als ob sie eines Beweises gar nicht bedürften, und sicherlich dadurch das zu beweisende Theorem zu einem hohen Grade von Wahrscheinlichkeit gebracht wird, sind sie doch, wenn geometrische Strenge gewünscht wird, keineswegs aufs Geratewohl zuzulassen. Was nun die Annahme in IV und V anlangt, dass es eine Primzahl r von der Form $4n+1$ giebt, welche von zwei andern gegebenen Primzahlen p, q Nichtrest ist, so folgt aus dem vierten Abschnitt leicht, dass alle Zahlen, welcher kleiner als $4pq$ und prim hierzu sind (deren Anzahl gleich $2(p-1)(q-1)$ ist), gleichmässig auf vier Klassen sich verteilen, von denen die eine die Nichtreste jeder der beiden Zahlen p, q, die drei übrigen aber die Reste von p und Nichtreste von q, die Nichtreste von p und Reste von q und die Reste jeder der beiden Zahlen p, q enthalten, und dass in den einzelnen Klassen die eine

Hälfte Zahlen von der Form $4n+1$, die andere Hälfte Zahlen von der Form $4n+3$ sind. Man hat daher unter jenen $\frac{1}{4}(p-1)(q-1)$ Nichtreste einer jeden der beiden Zahlen p, q von der Form $4n+1$, welche $g, g', g'', \ldots$ sein mögen, während die übrigen $\frac{3}{4}(p-1)(q-1)$ Zahlen $h, h', h'', \ldots$ seien. Offenbar werden alle in den Formen $4pqt+g$, $4pqt+g'$, $4pqt+g''$, ... enthaltenen Zahlen, deren Gesamtheit wir mit (G) bezeichnen, ebenfalls Nichtreste von p, q von der Form $4n+1$ sein. Nun ist klar, dass man zur Begründung der Annahme nur zu beweisen hat, dass unter den Formen (G) sicher Primzahlen enthalten sind; dies ist zwar an und für sich höchst wahrscheinlich, da diese Formen im Verein mit den Formen $4pqt+h$, $4pqt+h'$, ..., die wir mit (H) bezeichnen, alle zu $4pq$ primen Zahlen und daher auch alle absolut primen Zahlen (ausser $2, p, q$) enthalten und kein Grund vorhanden ist, warum nicht die Reihe der Primzahlen sich gleichmässig auf jene Formen verteilen sollte, so dass der achte Teil zu (G), die übrigen zu (H) gehören. Indessen ist offenbar eine solche Schlussweise von geometrischer Strenge weit entfernt. Legendre selbst giebt zu, dass der Beweis des Satzes, dass unter einer Form wie $kt+l$, wo k, l gegebene zu einander prime Zahlen sind und t eine unbestimmte Zahl bezeichnet, sicher Primzahlen enthalten seien, ziemlich schwierig erscheine, und giebt obenhin eine Methode an, die vielleicht dahin führen könnte. Es dürften jedoch, wie uns scheint, viele vorbereitende Untersuchungen notwendig sein, ehe man auf diesem Wege zu einem strengen Beweise gelangen kann. — Hinsichtlich der andern Annahme aber (III, zweite Methode), dass es eine Primzahl r von der Form $4n+3$ gebe, von welcher eine andere gegebene Primzahl p von der Form $4n+1$ Nichtrest ist, hat Legendre gar keine Bemerkung hinzugefügt. Wir haben oben (Artikel 129) bewiesen, dass es Primzahlen, von welchen p Nichtrest ist, sicher giebt, aber unsere Methode scheint nicht geeignet zu sein, um die Existenz solcher Primzahlen nachzuweisen, welche zugleich von der Form $4n+3$ sind (wie es hier, aber nicht in unserm ersten Beweise erforderlich ist). Übrigens können wir die Richtigkeit dieser Annahme leicht folgendermassen beweisen: Nach Artikel 287 giebt es ein positives Geschlecht binärer Formen mit der Determinante $-p$, dessen Character 3, 4; Np ist; es sei (a, b, c) eine solche Form und a ungerade (was man annehmen darf). Dann ist a von der Form $4n+3$ und entweder selbst prim oder wenigstens durch einen Primfactor von der Form $4n+3$ teilbar. Es ist aber $-pRa$ und daher auch $-pRr$, somit pNr. Man muss aber wohl beachten, dass die Sätze der Artikel 263, 287 sich auf das Fundamentaltheorem stützen, und es daher ein Zirkelschluss sein würde, wollte man einen Teil dieses Satzes auf jenen aufbauen. — Endlich ist die Annahme in der ersten Methode von III noch weit mehr aufs Geratewohl gemacht, so dass es nicht nötig ist, mehr darüber hier hinzuzufügen.

Es möge gestattet sein, in Betreff des Falles V, der nach der vorstehend angegebenen Methode zwar nicht bewiesen ist, aber doch durch

die folgende leicht erledigt wird, eine Bemerkung hinzuzufügen. Wenn daselbst gleichzeitig pNq, qNp wäre, so würde $-pRq$, $-qRp$ sein, woraus leicht folgt, dass -1 die characteristische Zahl der Form $(p, 0, q)$ ist, die sich somit (nach der Theorie der ternären Formen) durch die Form $x^2+y^2+z^2$ darstellen lässt. Ist

$$pt^2+qu^2=(\alpha t+\beta u)^2+(\alpha' t+\beta' u)^2+(\alpha'' t+\beta'' u)^2,$$

oder

$$\alpha^2+\alpha'^2+\alpha''^2=p, \quad \beta^2+\beta'^2+\beta''^2=q, \quad \alpha\beta+\alpha'\beta'+\alpha''\beta''=0,$$

so werden der ersten und zweiten Gleichung zufolge sämtliche $\alpha, \alpha', \alpha''$, β, β', β'' ungerade sein. Dann kann aber offenbar die dritte Gleichung nicht bestehen. — Auf ähnliche Weise lässt sich auch der Fall II erledigen.

298.

Aufgabe. Bezeichnen a, b, c beliebige Zahlen, so soll man die Bedingungen für die Lösbarkeit der Gleichung

$$(\omega) \qquad ax^2+by^2+cz^2=0$$

finden.

Auflösung. Es seien $\alpha^2, \beta^2, \gamma^2$ die grössten in bc, ac, ab resp. aufgehenden Quadrate, und es werde $\alpha a=\beta\gamma A$, $\beta b=\alpha\gamma B$, $\gamma c=\alpha\beta C$ gesetzt. Dann sind A, B, C zu einander prime ganze Zahlen; die Gleichung (ω) aber wird lösbar sein oder nicht, je nachdem die Gleichung

$$(\Omega) \qquad AX^2+BY^2+CZ^2=0$$

eine Lösung zulässt oder nicht, was nach Artikel 294 entschieden werden kann.

Beweis. Setzt man $bc=\mathfrak{A}\alpha^2$, $ac=\mathfrak{B}\beta^2$, $ab=\mathfrak{C}\gamma^2$, so werden $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ ganze, von quadratischen Factoren freie Zahlen und $\mathfrak{A}=BC$, $\mathfrak{B}=AC$, $\mathfrak{C}=AB$ sein. Hiernach ist $\mathfrak{A}\mathfrak{B}\mathfrak{C}=(ABC)^2$ und daher $ABC=A\mathfrak{A}=B\mathfrak{B}=C\mathfrak{C}$ notwendig ganz. Ist m der grösste gemeinschaftliche Teiler der Zahlen $\mathfrak{A}$, $A\mathfrak{A}$ und $\mathfrak{A}=gm$, $A\mathfrak{A}=hm$, so ist g prim zu h und auch (weil $\mathfrak{A}$ frei von jedem quadratischen Factor) zu m. Nun ist $h^2m=gA^2\mathfrak{A}=g\mathfrak{B}\mathfrak{C}$, und somit geht g in h^2m auf, was offenbar unmöglich ist, wenn nicht $g=\pm 1$ ist. Hiernach ist $\mathfrak{A}=\pm m$, $A=\pm h$ und somit eine ganze Zahl, und ebenso sind B und C ganze Zahlen. — Da $\mathfrak{A}=BC$ keine quadratischen Teiler hat, so müssen notwendig B und C prim zu einander sein; und ebenso ist A zu C und zu B prim. — Endlich ist klar, dass, wenn der Gleichung (Ω) durch $X=P$, $Y=Q$, $Z=R$ genügt wird, die Gleichung (ω) gelöst wird durch $x=\alpha P$, $y=\beta Q$, $z=\gamma R$, und umgekehrt, wenn dieser genügt wird durch $x=p$, $y=q$, $z=r$, so wird jene befriedigt durch $X=\beta\gamma p$, $Y=\alpha\gamma q$, $Z=\alpha\beta r$, so dass entweder jede der beiden Gleichungen oder keine von ihnen lösbar ist.

Darstellung der Null durch beliebige ternäre Formen.

299.

Aufgabe. Ist die ternäre Form

$$f = ax^2 + a'x'^2 + a''x''^2 + 2bx'x'' + 2b'xx'' + 2b''xx'$$

gegeben, so soll man finden, ob die Null durch sie dargestellt werden kann (durch Werte der Unbestimmten, welche nicht gleichzeitig gleich 0 sind).

Auflösung. I. Ist $a = 0$, so können die Werte von x', x'' beliebig angenommen werden, und aus der Gleichung

$$a'x'^2 + 2bx'x'' + a''x''^2 = -2x(b'x'' + b''x')$$

geht hervor, dass x einen bestimmten rationalen Wert erhält; so oft für x auf diese Weise ein Bruch sich ergiebt, braucht man nur die Werte von x, x', x'' mit dem Nenner des Bruches zu multiplicieren, wodurch man ganze Zahlen erhalten wird. Einzig und allein sind solche Werte von x', x'' auszuschliessen, für welche $b'x'' + b''x' = 0$ ist, falls sie nicht zu gleicher Zeit $a'x'^2 + 2bx'x'' + a''x''^2 = 0$ machen, in welchem Falle x nach Belieben angenommen werden kann. Zugleich ist klar, dass man auf diese Weise alle möglichen Lösungen erhalten kann. Übrigens gehört der Fall, in welchem $b' = b'' = 0$ ist, nicht hierher; denn dann kommt x in f garnicht vor oder f ist eine binäre Form und die Darstellbarkeit der Null durch f muss nach der Theorie derartiger Formen beurteilt werden.

II. Wenn aber a nicht gleich 0 ist, so ist der Gleichung $f = 0$ die folgende äquivalent:

$$(ax + b''x' + b'x'')^2 - A''x'^2 + 2Bx'x'' - A'x''^2 = 0,$$

wenn man setzt:

$$b''^2 - aa' = A'', \quad ab - b'b'' = B, \quad b'^2 - aa'' = A'.$$

Wenn nun hier $A' = 0$ aber nicht $B = 0$ ist, so werden offenbar, wenn $ax + b''x' + b'x''$ und x'' nach Belieben angenommen werden, x und x' daraus rational bestimmt, und falls sie nicht ganze Zahlen werden, so wird dadurch wenigstens ein passender Multiplicator bestimmt werden, welcher ganze Zahlen hervorbringt. Für einen einzigen Wert von x'', nämlich für $x'' = 0$ ist der Wert von $ax + b''x' + b'x''$ nicht willkürlich, sondern auch gleich 0 zu setzen; dann aber wird x' willkürlich angenommen werden können und wird einen rationalen Wert von x ergeben. Wenn dagegen gleichzeitig $A'' = 0$ und $B = 0$ ist, so ist klar, dass, wenn A' ein Quadrat $= k^2$ ist, die Gleichung $f = 0$ zurückkommt auf die folgenden beiden linearen (von denen entweder die eine oder die andere stattfinden muss):

$$ax + b''x' + (b' + k)x'' = 0, \quad ax + b''x' + (b' - k)x'' = 0;$$

ist dagegen (unter derselben Voraussetzung) A' eine nichtquadratische Zahl, so hängt offenbar die Lösung der gegebenen Gleichung ab von den folgenden: $x''=0$ und $ax+b''x'=0$ (welche gleichzeitig stattfinden müssen).

Übrigens wird es kaum nötig sein zu bemerken, dass die Methode in I auch angewendet werden kann, wenn a' oder a'' gleich 0, und die Methode in II, wenn $A'=0$ ist.

III. Wenn aber weder a noch A'' gleich 0 ist, so ist der Gleichung $f=0$ die folgende äquivalent:

$$A''(ax+b''x'+b'x'')^2-(A''x'-Bx'')^2+Dax''^2=0,$$

wenn man mit D die Determinante der Form f oder mit Da die Zahl $B^2-A'A''$ bezeichnet. Ist $D=0$, so wird sich die Auflösung in ähnlicher Weise verhalten wie am Schlusse des vorigen Falles; ist nämlich A'' ein Quadrat und zwar gleich k^2, so reduciert sich die gegebene Gleichung auf die folgenden:

$$kax+(kb''-A'')x'+(kb'+B)x''=0,\quad kax+(kb''+A'')x'+(kb''-B)x''=0;$$

ist aber A'' kein Quadrat, so muss

$$ax+b''x'+b'x''=0,\quad A''x'-Bx''=0$$

gesetzt werden. — Wenn dagegen D nicht gleich 0 ist, so werden wir zu der Gleichung geführt:

$$A''t^2-u^2+Dav^2=0,$$

deren Möglichkeit nach dem vorigen Artikel beurteilt werden kann. Wenn nun diese nicht anders gelöst werden kann als durch $t=0$, $u=0$, $v=0$, so wird offenbar auch die gegebene Gleichung keine andere Lösung besitzen, als $x=0$, $x'=0$, $x''=0$; wenn aber jene auf andere Weise lösbar ist, so ergeben sich aus irgend welchen Werten von t, u, v mittelst der Gleichungen

$$ax+b''x'+b'x''=t,\quad A''x'-Bx''=u,\quad x''=v$$

wenigstens rationale Werte von x, x', x'', aus denen man, wenn sie Brüche enthalten, mittelst eines passenden Multiplicators ganzzahlige Werte ableiten kann.

Sobald aber eine einzige Lösung der Gleichung $f=0$ in ganzen Zahlen gefunden ist, lässt sich die Aufgabe auf den Fall I zurückführen und es können ebenso wie dort sämtliche Lösungen dargestellt werden. Dies geschieht in folgender Weise. Es mögen der Gleichung $f=0$ die Werte α, α', α'' von x, x', x'', die wir als frei von gemeinschaftlichen Factoren voraussetzen, genügen; man nehme ferner (gemäss Artikel 40 und 279) ganze Zahlen β, β', β'', γ, γ', γ'' so an, dass

$$\alpha(\beta'\gamma''-\beta''\gamma')+\alpha'(\beta''\gamma-\beta\gamma'')+\alpha''(\beta\gamma'-\beta'\gamma)=1$$

ist, und es gehe f durch die Substitution

$$(S)\ x=\alpha y+\beta y'+\gamma y'',\quad x'=\alpha' y+\beta' y'+\gamma' y'',\quad x''=\alpha'' y+\beta'' y'+\gamma'' y''$$

in die Form

$$g = cy^2 + c'y'^2 + c''y''^2 + 2dy'y'' + 2d'y''y + 2d''yy'$$

über. Dann wird offenbar $c = 0$ und g der Form f äquivalent sein, woraus leicht folgt, dass sich aus allen Lösungen der Gleichung $G = 0$ (vermittelst der Substitution S) sämtliche ganzzahligen Lösungen der Gleichung $f = 0$ ergeben. Nun folgt aus I, dass sämtliche Lösungen der Gleichung $g = 0$ enthalten sind unter den Formeln:

$$y = -z(c'p^2 + 2dpq + c''q^2), \quad y' = 2z(d''p^2 + d'pq), \quad y'' = 2z(d''pq + d'q^2),$$

wo p, q unbestimmte ganze Zahlen, z eine unbestimmte Zahl bezeichnet, für welche auch Brüche genommen werden können, wofern nur y, y', y'' ganze Zahlen bleiben. Setzt man diese Werte von y, y', y'' in (S) ein, so erhält man sämtliche ganzzahligen Lösungen der Gleichung $f = 0$.

So ergiebt sich z. B. wenn

$$f = x^2 + x'^2 + x''^2 - 4x'x'' + 2xx'' + 8xx'$$

und eine Lösung der Gleichung $f = 0$ durch $x = 1$, $x' = -2$, $x'' = 1$ gegeben ist, indem man $\beta, \beta', \beta'', \gamma, \gamma', \gamma''$ respective gleich 0, 1, 0, 0, 0, 1 setzt:

$$g = y'^2 + y''^2 - 4y'y'' + 12yy''.$$

Hiernach werden alle ganzzahligen Lösungen der Gleichung $g = 0$ unter der Formel

$$y = -z(p^2 - 4pq + q^2), \quad y' = 12zpq, \quad y'' = 12zq^2,$$

und somit sämtliche Lösungen der Gleichung $f = 0$ unter der folgenden enthalten sein:

$$\begin{aligned} x &= -z(p^2 - 4pq + q^2) \\ x' &= 2z(p^2 + 2pq + q^2) \\ x'' &= -z(p^2 - 4pq - 11q^2). \end{aligned}$$

Allgemeine Lösung der unbestimmten Gleichungen zweiten Grades mit zwei Unbekannten durch rationale Grössen.

300.

Aus der Aufgabe des vorigen Artikels ergiebt sich von selbst die Lösung der unbestimmten Gleichung:

$$ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0,$$

wenn nur rationale Werte verlangt werden; dieselbe Gleichung haben wir, wenn ganze Zahlen gefordert werden, schon oben (Artikel 216 u. ff.) erledigt. Denn alle rationalen Werte von x, y können dargestellt werden durch $\frac{t}{v}$, $\frac{u}{v}$ derart, dass t, u, v ganze Zahlen sind, woraus hervorgeht,

dass die Lösung jener Gleichung durch rationale Zahlen identisch ist mit der Lösung der Gleichung

$$at^2 + 2btu + cu^2 + 2dtv + 2euv + fv^2 = 0$$

in ganzen Zahlen; diese stimmt aber mit der im vorigen Artikel behandelten Gleichung überein. Ausgeschlossen müssen nur diejenigen Lösungen werden, in denen $v = 0$ ist; solche kann es aber nicht geben, wenn $b^2 - ac$ eine nichtquadratische Zahl ist. So sind z. B. alle Lösungen der (im Artikel 221 durch ganze Zahlen allgemein gelösten) Gleichung

$$x^2 + 8xy + y^2 + 2x - 4y + 1 = 0$$

durch rationale Zahlen enthalten unter der Formel:

$$x = \frac{p^2 - 4pq + q^2}{p^2 - 4pq - 11q^2}, \quad y = -\frac{2p^2 + 4pq + 2q^2}{p^2 - 4pq - 11q^2},$$

wo p, q irgend welche ganzen Zahlen bezeichnen. — Übrigens haben wir hier über diese beiden in engstem Zusammenhange stehenden Aufgaben nur kurz gehandelt und viele hierauf bezügliche Bemerkungen unterdrückt, einerseits um nicht zu weitläufig zu werden, andererseits weil wir im Besitze einer andern auf allgemeineren Prinzipien beruhenden Auflösung der Aufgabe des vorigen Artikels sind, deren Auseinandersetzung wir uns auf eine andere Gelegenheit aufsparen müssen, da dieselbe eine eingehendere Untersuchung der ternären Formen erfordert.

Über die mittlere Anzahl der Geschlechter.

301.

Wir kehren zu den binären Formen zurück, von denen wir noch mehrere besondere Eigenschaften anführen müssen. Zunächst werden wir einige Bemerkungen in Bezug auf die Anzahl der Geschlechter und Klassen in einer eigentlich primitiven (für eine negative Determinante: positiven) Ordnung, auf welche wir der Kürze wegen die Untersuchung beschränken, hinzufügen.

Die Anzahl der Geschlechter, in welche sämtliche (eigentlich primitive positive) Formen mit gegebener positiver oder negativer Determinante $\pm D$ zerfallen, ist stets gleich 1, 2, 4 oder gleich einer höheren Potenz der Zahl 2, deren Exponent von den Factoren von D abhängt und nach den vorstehenden Untersuchungen ganz *a priori* gefunden werden kann. Da nun in der natürlichen Zahlenreihe Primzahlen mit mehr oder weniger zusammengesetzten Zahlen vermischt sind, geschieht es, dass für mehrere aufeinanderfolgende Determinanten $\pm D$, $\pm(D+1)$, $\pm(D+2)$, ... die Anzahl der Geschlechter bald zunimmt bald abnimmt und in dieser verworrenen Reihe keine Ordnung zu herrschen scheint. Trotzdem ergiebt sich, wenn man die

Anzahlen der Geschlechter, welche vielen aufeinanderfolgenden Determinanten

$$\pm D, \quad \pm(D+1), \ldots, \quad \pm(D+m)$$

entsprechen, addiert und die Summe durch die Anzahl der Determinanten dividiert, eine **mittlere Geschlechteranzahl**, welche als für die mittlere der Determinanten $\pm(D+\frac{1}{2}m)$ stattfindend angesehen werden kann und eine sehr reguläre Reihe bildet. Wir nehmen aber an, nicht nur dass m hinreichend gross, sondern auch, dass D noch weit grösser ist, damit das Verhältnis der äussersten Determinanten D, $D+m$ nicht zu sehr vom Verhältnis der Gleichheit abweicht. Die Regelmässigkeit jener Reihe ist folgendermassen zu verstehen: Ist D' eine Zahl, die um vieles grösser ist als D, so wird die mittlere Anzahl der Geschlechter in Bezug auf die Determinante $\pm D'$ erheblich grösser sein, als in Bezug auf D; wenn aber D, D' nicht sehr verschieden sind, so werden auch die mittleren Anzahlen der Geschlechter in Bezug auf D und D' nahezu gleich sein. Übrigens findet man die mittlere Anzahl der Geschlechter in Bezug auf die positive Determinante $+D$ stets gleich der mittleren Anzahl der Geschlechter in Bezug auf die negative $-D$ und zwar um so genauer, je grösser D ist, während für einen kleinen Wert die erstere ein wenig grösser wird, als die letztere. Diese Bemerkungen werden deutlicher durch folgende Beispiele, welche wir einer mehr als 4000 Determinanten umfassenden Tafel der Klasseneinteilung der binären Formen entnommen haben. Unter den hundert Determinanten von 801 bis 900 finden sich 7, denen nur ein einziges Geschlecht entspricht; 32, 52, 8, 1, denen respective 2, 4, 8, 16 Geschlechter entsprechen; daher ergeben sich im Ganzen 359 Geschlechter, so dass die mittlere Anzahl gleich 3, 59 ist. Die hundert negativen Determinanten von -801 bis -900 ergeben 360 Geschlechter. Die folgenden Beispiele sind sämtlich von negativen Determinanten hergenommen. Im sechzehnten Hundert (von -1501 bis -1600) findet sich als mittlere Geschlechteranzahl die Zahl 3, 89; im fünfundzwanzigsten Hundert ist sie 4, 03, im einundfünfzigsten 4, 24; aus den sechshundert Determinanten von -9401 bis -10000 ergiebt sich die Zahl 4, 59. Aus diesen Beispielen geht hervor, dass die mittlere Geschlechteranzahl weit langsamer zunimmt, als die Determinanten selbst. Aber, fragt man, welches ist denn nun das Gesetz dieser Reihe? — Durch eine ziemlich schwierige theoretische Untersuchung, die hier darzulegen allzu weitläufig sein würde, wurde gefunden, dass die mittlere Geschlechteranzahl für die Determinante $+D$ oder $-D$ möglichst nahe durch die Formel

$$\alpha \log D + \beta$$

dargestellt werden kann, wo α, β constante Grössen sind und zwar:

$$\alpha = \frac{4}{\pi^2} = 0{,}4052847346$$

(wo π den halben Umfang eines Kreises mit dem Radius 1 bezeichnet),

$$\beta = 2\alpha g + 3\alpha^2 h - \tfrac{1}{6}\alpha \log 2 = 0{,}8830460462,$$

wo g die Summe der Reihe

$$1 - \log(1+1) + \tfrac{1}{2} - \log(1+\tfrac{1}{2}) + \tfrac{1}{3} - \log(1+\tfrac{1}{3}) + \cdots = 0{,}5772156649$$

(vgl. Euler, *Inst. Calc. Diff. p. 444*), h aber die Summe der Reihe

$$\tfrac{1}{4}\log 2 + \tfrac{1}{9}\log 3 + \tfrac{1}{16}\log 4 + \cdots\cdot$$

ist, welche näherungsweise gleich 0,9375482543 gefunden wurde. Aus dieser Formel geht hervor, dass die mittlere Anzahl der Geschlechter in arithmetischer Reihe zunimmt, wenn die Determinanten in geometrischer Reihe wachsen. Als Werte dieser Formel für $D = 850\frac{1}{2}, 1550\frac{1}{2}, 2450\frac{1}{2}, 5050\frac{1}{2}, 9700\frac{1}{2}$ findet man bezüglich 3, 617; 3, 86; 4, 046; 4, 339; 4, 604, welche von den oben angegebenen mittleren Anzahlen nur sehr wenig abweichen. Je grösser die mittlere Determinante ist und aus je mehr Determinanten die mittlere Anzahl berechnet wird, um so weniger wird sie sich von dem Werte, den die Formel giebt, unterscheiden. Mit Hülfe dieser Formel kann auch das Aggregat der den aufeinanderfolgenden Determinanten $\pm D, \pm(D+1), \ldots, \pm(D+m)$ entsprechenden Geschlechteranzahlen annähernd ermittelt werden, wenn man die den einzelnen Determinanten entsprechenden mittleren Anzahlen berechnet und summiert, wie sehr verschieden auch die äussersten Determinanten $D, D+m$ sein mögen. Diese Summe ist gleich

$$\alpha\,[log D + log\,(D+1) + log\,(D+2) + \cdots\cdot + log\,(D+m)] + \beta\,(m+1)$$

oder hinreichend genau gleich

$$\alpha\,[(D+m)\,log\,(D+m) - (D-1)\,log\,(D-1)] + (\beta - \alpha)\,(m+1).$$

Auf diese Weise findet man die Summe der Geschlechteranzahlen für die Determinanten -1 bis -100 gleich 234, 4, während sie in Wirklichkeit gleich 233 ist; analog von -1 bis -2000 gleich 7116, 6, während sie in Wirklichkeit gleich 7112 ist; von -1 bis -3000 ergiebt die Tafel die Zahl 11166, die Formel 11167, 9; von -9001 bis -10000, wo jene Summe gleich 4595 ist, ergiebt die Formel 4594, 9, eine Übereinstimmung, wie sie kaum erwartet werden konnte.

Über die mittlere Anzahl der Klassen.

302.

Hinsichtlich der Anzahl der Klassen (eigentlich primitiven positiven, was immer hinzuzudenken ist) verhalten sich die positiven Determinanten ganz anders als die negativen; deshalb werden wir beide gesondert betrachten. Darin stimmen diese mit jenen überein, dass für eine gegebene Determinante in den einzelnen Geschlechtern gleichviel Klassen enthalten sind und daher die Anzahl aller Klassen gleich ist dem Product aus der Anzahl der Geschlechter und der Anzahl der in jedem einzelnen Geschlechte enthaltenen Klassen.

Was zunächst die negativen Determinanten angeht, so bildet die Anzahl der mehreren aufeinanderfolgenden Determinanten $-D, -(D+1), -(D+2), \ldots$ entsprechenden Klassen eine ebenso verworrene Reihe, wie die Anzahl der Geschlechter. Die mittlere Klassenzahl aber (für die eine Erklärung nicht nötig ist) wächst sehr regelmässig, wie aus den folgenden Beispielen erhellen wird. Die hundert Determinanten von -500 bis -600 ergeben 1729 Klassen, so dass die mittlere Anzahl gleich 17, 29 ist. Ebenso findet man in dem fünfzehnten Hundert als mittlere Klassenzahl 28, 26; aus dem 24. und 25. Hundert ergiebt sich die Zahl 36, 28, aus dem 61., 62. und 63. Hundert die Zahl 58, 50, aus dem 91. bis 95. Hundert die Zahl 71, 56, endlich aus dem 96. bis 100. Hundert die Zahl 73, 54. Diese Beispiele zeigen, dass die mittlere Klassenanzahl zwar langsamer wächst als die Determinanten, aber doch viel schneller als die mittlere Geschlechteranzahl; bei nur mässiger Aufmerksamkeit erkennt man, dass jene ziemlich genau im Verhältnis der Quadratwurzeln aus den mittleren Determinanten wächst. In der That haben wir durch eine theoretische Untersuchung gefunden, dass die mittlere Klassenanzahl in Bezug auf die Determinante $-D$ sehr nahe ausgedrückt wird durch

$$\gamma\sqrt{D} - \delta,$$

wo

$$\gamma = 0{,}7467183115 = \frac{2\pi}{7e},$$

e die Summe der Reihe

$$1 + \frac{1}{8} + \frac{1}{27} + \frac{1}{64} + \frac{1}{125} + \cdots$$

und

$$\delta = 0{,}2026423673 = \frac{2}{\pi^2}$$

ist. Die nach dieser Formel berechneten mittleren Werte weichen von denjenigen, welche wir oben der Tafel für die Klasseneinteilung entnommen haben, nur sehr wenig ab. Mit Hülfe dieser Formel kann man auch das Aggregat der Anzahl aller (eigentlich primitiven positiven) Klassen, welche den aufeinanderfolgenden Determinanten $-D, -(D+1), -(D+2), \ldots, -(D+m-1)$ entsprechen, näherungsweise angeben, wie weit auch die äusseren Determinanten von einander verschieden sein mögen, indem man die jenen Determinanten nach der Formel entsprechenden mittleren Klassenanzahlen summiert. Man erhält so dasselbe gleich

$$\gamma[\sqrt{D} + \sqrt{D+1} + \cdots + \sqrt{D+m-1}] - \delta m$$

oder näherungsweise gleich

$$\tfrac{2}{3}\gamma[\sqrt{D+m-\tfrac{1}{2}}^{\,3} - \sqrt{D-\tfrac{1}{2}}^{\,3}] - \delta m.$$

So ergiebt sich z. B. für die hundert Determinanten von -1 bis -100 jenes Aggregat nach der Formel gleich 481, 1, während es in

Wirklichkeit gleich 477 ist; die tausend Determinanten —1 bis —1000 ergeben nach der Tafel 15 533 Klassen, die Formel giebt 15 551,4; das zweite Tausend enthält nach der Tafel 28 595 Klassen, die Formel liefert 28 585,7; ebenso enthält das dritte Tausend in Wirklichkeit 37 092 Klassen, während die Formel 37 074,3 giebt; das zehnte Tausend giebt 72 549 nach der Tafel, während die Formel 72 572 liefert.

303.

Eine Tafel der negativen Determinanten, welche nach der Verschiedenheit der ihnen entsprechenden Klasseneinteilungen aufgestellt ist, giebt noch zu vielen andern besonderen Bemerkungen Anlass. Für die Determinanten von der Form $-(8n+3)$ ist die Anzahl der Klassen (sowohl derjenigen, welche in sämtlichen Geschlechtern, als auch derjenigen, welche in den einzelnen eigentlich primitiven Geschlechtern enthalten sind) stets durch 3 teilbar, die einzige Determinante —3 ausgenommen, wofür der Grund aus Artikel 256, VI von selbst sich ergiebt. Für diejenigen Determinanten, deren Formen nur ein einziges Geschlecht ausmachen, ist die Anzahl der Klassen immer ungerade; denn da es für eine solche Determinante nur eine einzige ambige Klasse giebt, nämlich die Hauptklasse, so ist die Anzahl aller übrigen Klassen, von denen stets je zwei entgegengesetzt sind, notwendig gerade, und daher die Anzahl aller ungerade; übrigens gilt diese letztere Eigenschaft auch für positive Determinanten. — Ferner scheint die Reihe der Determinanten, denen dieselbe gegebene Klasseneinteilung (d. h. eine gegebene Anzahl sowohl von Geschlechtern als auch von Klassen) entspricht, stets abzubrechen, welche ziemlich seltsame Bemerkung wir durch einige Beispiele erläutern. (Die erste, römische, Zahl zeigt die Anzahl der eigentlich primitiven positiven Geschlechter, die folgende die Anzahl der in jedem einzelnen Geschlechte enthaltenen Klassen an; dann folgt die Reihe der Determinanten, welchen jene Klassifikation entspricht, und deren negatives Vorzeichen wir der Kürze wegen weggelassen haben.)

I. 1	1, 2, 3, 4, 7
II. 3	11, 19, 23, 27, 31, 43, 67, 163
I. 5	47, 79, 103, 127
I. 7	71, 151, 223, 343, 463, 487
II. 1	5, 6, 8, 9, 10, 12, 13, 15, 16, 18, 22, 25, 28, 37, 58
II. 2	14, 17, 20, 32, 34, 36, 39, 46, 49, 52, 55, 63, 64, 73, 82, 97, 100, 142, 148, 193
IV. 1	21, 24, 30, 33, 40, 42, 45, 48, 57, 60, 70, 72, 78, 85, 88, 93, 102, 112, 130, 133, 177, 190, 232, 253
VIII. 1	105, 120, 165, 168, 210, 240, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760
XVI. 1	840, 1320, 1365, 1848.

Analog finden sich 20 Determinanten (deren grösste gleich —1423 ist), welchen die Klassifikation I. 9 entspricht; 4 (die grösste gleich —1303), welchen die Klassifikation I. 11 entspricht, u. s. w. Die Klassifikationen II. 3, II. 4, II. 5, IV. 2 entsprechen nicht mehr als 48, 31, 44, 69 Determinanten respective, von denen die grössten —652, —862, —1318, —1012 sind. Da die Tafel, aus welcher diese Beispiele entnommen sind, weit über die grössten hier vorkommenden Determinanten hinaus fortgesetzt ist*), so scheint es nicht zweifelhaft zu sein, dass die hingeschriebenen Reihen in der That abbrechen und diesen Schluss werden wir der Analogie gemäss auch auf beliebige andere Klassifikationen ausdehnen dürfen. Da z. B. im ganzen zehnten Tausend der Determinanten sich keine findet, welcher eine Klassenzahl unterhalb 24 entspräche, so ist es höchstwahrscheinlich, dass die Klassifikationen I. 23; I. 21; ..., II. 11, II. 10, ..., IV. 5, IV. 4, IV. 3, VIII. 2 schon vor —9000 aufgehört haben oder wenigstens nur sehr wenigen Determinanten jenseits von —10000 zukommen. Die strengen Beweise dieser Bemerkungen aber scheinen sehr schwierig zu sein. Nicht minder merkwürdig ist es, dass sämtliche Determinanten, deren Formen in 32 oder mehr Geschlechter zerfallen, mindestens je zwei Klassen in den einzelnen Geschlechtern haben, und daher die Klassifikationen XXXII. 1, LXIV, 1, u. s. w. gänzlich ausfallen (der kleinsten von diesen Determinanten, —9240, entspricht XXXII. 2), und es erscheint ziemlich wahrscheinlich, dass mit wachsender Geschlechteranzahl fortwährend mehr Klassifikationen ausfallen. In dieser Hinsicht sind die oben angeführten 65 Determinanten, welchen die Klassifikationen I. 1, II. 1, IV. 1, VIII. 1, XVI. 1 entsprechen, höchst bemerkenswert und man sieht leicht, dass sie sämtlich und zwar sie allein die beiden ausgezeichneten Eigenschaften besitzen, dass sämtliche zu ihnen gehörigen Formenklassen ambig und irgend zwei in demselben Geschlechte enthaltene Formen notwendig sowohl eigentlich als auch uneigentlich äquivalent sind. Übrigens sind dieselben 65 Zahlen (unter einem etwas verschiedenen Gesichtspunkte, dessen unten Erwähnung gethan werden wird, und mit einem leicht zu beweisenden Kriterium) schon von Euler angegeben worden, *Nouv. Mém. de l'Ac. de Berlin 1776 p. 338.*

304.

Die Anzahl der eigentlich primitiven Klassen, welche die binären Formen mit positiver quadratischer Determinante k^2 bilden, kann überhaupt *a priori* bestimmt werden und ist gleich der Anzahl der Zahlen, welche prim zu $2k$ und kleiner als $2k$ sind; daraus leitet man durch nicht schwierige Schlüsse, die wir hier unterdrücken müssen, her, dass die mittlere

*) Nämlich während des Druckes der *Disquisitiones* bis zu —3000 in einem Zuge, sodann durch das ganze zehnte Tausend und mehrere andere zerstreute Hunderte, zu denen noch sehr viele besondere mit Fleiss ausgewählte Determinanten kommen.

Anzahl der zu solchen Determinanten gehörigen Klassen für die Determinante k^2 sehr nahe durch $\frac{8k}{\pi^2}$ ausgedrückt wird. — Die positiven nichtquadratischen Determinanten aber bieten in dieser Hinsicht ganz eigenartige Erscheinungen dar. Während nämlich eine kleine Klassenanzahl, z. B. die Klassifikation I. 1 oder I. 3 oder II. 1 u. s. w., bei negativen und quadratischen Determinanten nur für kleine, sich nicht weit erstreckende Werte derselben stattfindet, besitzt dagegen unter den positiven nichtquadratischen Determinanten, wenigstens wenn sie nicht sehr gross sind, der bei weitem grösste Teil solche Klassifikationen, wo nur eine Klasse in jedem Geschlechte vorhanden ist, so dass die folgenden I. 3, I. 5, II. 2, II. 3, IV. 2 u. s. w. sehr selten sind. So befinden sich z. B. unter den 90 nichtquadratischen, die Zahl 100 nicht übersteigenden Determinanten 11, 48, 27, welchen die Klassifikationen I. 1; II. 1; IV. 1 respective entsprechen; nur für eine einzige (37) ist I. 3, zwei (34 und 82) haben die Klassifikation II. 2 und nur eine (79) die Klassifikation II. 3. Wenn jedoch die Determinanten zunehmen, so werden grössere Klassenanzahlen merklich häufiger; so besitzen z. B. unter den 96 nichtquadratischen Determinanten von 101 bis 200 zwei (101 und 197) die Klassifikation I. 3; vier (nämlich 145, 146, 178, 194) die Klassifikation II. 2; drei (141, 148, 189) die folgende: II. 3. Von den 197 nichtquadratischen Determinanten von 801 bis 1000 haben drei die Klassifikation I. 3, vier II. 2, vierzehn II. 3, zwei II. 5, zwei II. 6, fünfzehn IV. 2, sechs IV. 3, zwei IV. 4, vier VIII. 2; die übrigen 145 haben nur eine Klasse in jedem Geschlechte. — Es würde eine schöne und der Anstrengung der Geometer nicht unwürdige Aufgabe sein, zu ermitteln, nach welchem Gesetze die nur eine Klasse in jedem Geschlechte besitzenden Determinanten fortwährend seltener werden; bis jetzt können wir weder theoretisch entscheiden, noch durch Beobachtung mit hinreichender Sicherheit vermuten, ob dieselben endlich ganz abbrechen (was jedoch wenig wahrscheinlich erscheint), oder wenigstens unendlich selten werden, oder ob ihre Häufigkeit sich beständig mehr einer festen Grenze nähert. Die mittlere Klassenanzahl wächst in einem nur wenig grösseren Verhältnis als die Anzahl der Geschlechter, und bei weitem langsamer als die Quadratwurzeln aus den Determinanten; zwischen 800 und 1000 findet man jene gleich 5,01. Es möge gestattet sein, diesen Bemerkungen eine andere hinzuzufügen, welche die Analogie zwischen den positiven und negativen Determinanten in gewisser Weise wiederherstellt. Wir finden nämlich, dass für eine positive Determinante D nicht sowohl die Klassenanzahl selbst als vielmehr das Product aus dieser Anzahl und dem Logarithmus der Grösse $t + u\sqrt{D}$ (wo t, u die kleinsten der Gleichung $t^2 - Du^2 = 1$ genügenden Zahlen ausser 1,0 bezeichnen) der Klassenanzahl für eine negative Determinante aus mehreren hier nicht weitläufiger darzulegenden Gründen analog ist, und dass der mittlere Wert jenes Products ebenso genau durch eine Formel von der Form $m\sqrt{D} - n$ dargestellt wird; doch vermochten wir noch nicht die Werte der

constanten Grössen m, n' theoretisch zu bestimmen. Wenn man aus der Vergleichung einiger Hunderte von Determinanten etwas folgern darf, so scheint der Wert von m nicht sehr von $2\frac{1}{3}$ verschieden zu sein. — Übrigens behalten wir uns vor, über die Prinzipien der vorstehenden Untersuchungen betreffend die mittleren Werte von Grössen, welche nicht nach einem analytischen Gesetze fortschreiten, sondern sich nur einem solchen Gesetze asymptotisch fortwährend nähern, bei anderer Gelegenheit ausführlicher zu handeln. Wir gehen jetzt zu einer andern Untersuchung über, durch welche verschiedene eigentlich primitive Klassen mit derselben Determinante mit einander verglichen werden, womit wir dann diesen langen Abschnitt beschliessen.

Eigentümlicher Algorithmus der eigentlich primitiven Klassen; reguläre und irreguläre Determinanten u. s. w.

305.

Satz. Bezeichnet K die Hauptklasse der Formen mit der gegebenen Determinante D, C irgend eine andere Klasse aus dem Hauptgeschlecht der Formen mit derselben Determinante, sind endlich $2C$, $3C$, $4C$, ... die Klassen, welche durch Duplikation, Triplikation, Quadruplikation u. s. w. der Klasse C (wie im Artikel 249) entstehen, so wird man in der Reihe $C, 2C, 3C, \ldots$, wenn sie weit genug fortgesetzt wird, endlich zu einer Klasse, die mit K identisch ist, gelangen, und nimmt man an, dass mC die erste mit K identische Klasse und die Anzahl aller im Hauptgeschlechte enthaltenen Klassen gleich n sei, so ist entweder $m = n$ oder m ein aliquoter Teil von n.

Beweis. I. Da sämtliche Klassen $K, C, 2C, 3C, \ldots$ notwendig zum Hauptgeschlechte gehören (Artikel 247), so können die $n+1$ ersten Klassen dieser Reihe $K, C, 2C, \ldots, nC$ offenbar nicht sämtlich verschieden sein. Es wird daher entweder K mit irgend einer der Klassen $C, 2C, 3C, \ldots, nC$ identisch, oder es werden wenigstens zwei von diesen Klassen unter sich identisch sein. Es sei $rC = sC$ und $r > s$; dann ist auch:

$$(r-1)\,C = (s-1)\,C,\;\; (r-2)\,C = (s-2)\,C, \ldots,\;\; (r+1-s)\,C = C,$$

somit $(r-s)\,C = K$.

II. Hieraus folgt auch sogleich, dass m entweder $= n$ oder $< n$ ist, und es bleibt daher nur zu zeigen, dass im letzteren Falle m ein aliquoter Teil von n ist. Da die Klassen

$$K,\; C,\; 2C, \ldots, (m-1)\,C,$$

deren Complex wir mit $\mathfrak{C}$ bezeichnen, in diesem Falle das ganze Haupt-

geschlecht noch nicht erschöpfen, so sei C' irgend eine in $\mathfrak{C}$ nicht enthaltene Klasse dieser Art, und es werde der Complex der Klassen, welche durch Composition von C' mit den einzelnen Klassen in $\mathfrak{C}$ entstehen, nämlich

$$C',\ C' + C,\ C' + 2C, \ldots,\ C' + (m-1)\,C,$$

mit $\mathfrak{C}'$ bezeichnet. Man sieht nun leicht, dass alle Klassen in C' sowohl unter einander als auch von sämtlichen Klassen in $\mathfrak{C}$ verschieden sind und zum Hauptgeschlechte gehören. Wenn daher $\mathfrak{C}$ und $\mathfrak{C}'$ dieses Geschlecht völlig erschöpfen, so haben wir $n = 2m$, wenn nicht, so ist $2m < n$. Es sei im letzteren Falle C'' irgend eine andere weder in $\mathfrak{C}$ noch in $\mathfrak{C}'$ enthaltene Klasse des Hauptgeschlechts und man bezeichne die Gesamtheit der Klassen, welche durch Composition von C'' mit den einzelnen Klassen in $\mathfrak{C}$ hervorgehen, nämlich

$$C'',\ C'' + C,\ C'' + 2C, \ldots,\ C'' + (m-1)\,C,$$

mit $\mathfrak{C}''$. Dann folgt leicht, dass alle diese unter sich und von sämtlichen Klassen in $\mathfrak{C}$ und $\mathfrak{C}'$ verschieden sind und zum Hauptgeschlechte gehören. Wenn daher $\mathfrak{C}, \mathfrak{C}', \mathfrak{C}''$ dieses Geschlecht erschöpfen, so ist $n = 3m$, wenn nicht, so ist $n > 3m$, in welchem Falle eine andere in dem Hauptgeschlechte, aber nicht in $\mathfrak{C}, \mathfrak{C}'$ oder $\mathfrak{C}''$ enthaltene Klasse, wenn sie auf ähnliche Weise behandelt wird, zu dem Schlusse führt, dass entweder $n = 4m$ oder $n > 4m$ ist, u. s. f. Da nun n und m endliche Zahlen sind, so wird das Hauptgeschlecht notwendig einmal erschöpft werden, und es wird n ein Vielfaches von m oder m ein aliquoter Teil von n sein.

Beispiel. Ist $D = -356$, $C = (5, 2, 72)$*), so findet man: $2C = (20, 8, 21)$, $3C = (4, 0, 89)$, $4C = (20, -8, 21)$, $5C = (5, -2, 72)$, $6C = (1, 0, 356)$. Hier ist also $m = 6$, n aber ist für diese Determinante gleich 12. Nimmt man für C' die Klasse $(8, 2, 45)$, so sind die übrigen fünf Klassen in C': $(9, -2, 40)$, $(9, 2, 40)$, $(8, -2, 45)$, $(17, 1, 21)$, $(17, -1, 21)$.

306.

Man wird finden, dass der Beweis des vorstehenden Satzes ganz analog ist den Beweisen in den Artikeln 45, 49, und in der That besitzt die Theorie der Multiplikation der Klassen mit dem im dritten Abschnitt behandelten Gegenstande in jeder Beziehung einen sehr nahen Zusammenhang. Doch gestatten die Grenzen dieses Werkes nicht, jene Theorie mit der ihr gebührenden Ausführlichkeit zu verfolgen; wir fügen daher hier nur einige Bemerkungen hinzu, unterdrücken auch die Beweise, welche einen weitläufigeren Apparat erfordern würden, und behalten uns eine ausführlichere Untersuchung für eine andere Gelegenheit vor.

*) Die Klassen werden hier immer durch die (einfachsten) in ihnen enthaltenen Formen dargestellt.

I. Wird die Reihe $K, C, 2C, 3C, \ldots$ über $(m-1)\,C$ hinaus fortgesetzt, so werden sich wiederum dieselben Klassen ergeben:

$$mC = K,\ (m+1)\,C = C,\ (m+2)\,C = 2C, \ldots$$

und allgemein werden (wenn man der Kürze wegen K als $0C$ betrachtet) die Klassen gC, $g'C$ identisch oder verschieden sein, je nachdem g und g' nach dem Modul m congruent oder incongruent sind. Die Klasse nC ist daher immer identisch mit der Hauptklasse K.

II. Die Gesamheit der Klassen $K, C, 2C, \ldots, (m-1)\,C$, welche wir oben mit $\mathfrak{C}$ bezeichnet haben, werden wir die **Periode der Klasse** C nennen, welcher Ausdruck nicht mit den in den Artikeln 186 u. ff. behandelten Perioden der reducierten Formen mit positiver nichtquadratischer Determinante zu verwechseln ist. Offenbar entsteht also durch Composition beliebig vieler in derselben Periode enthaltenen Klassen ebenfalls eine in dieser Periode enthaltene Klasse:

$$gC + g'C + g''C + \cdots = (g + g' + g'' + \cdots)\,C.$$

III. Da $C + (m-1)\,C = K$ ist, so werden die Klassen C und $(m-1)\,C$ und ebenso $2C$ und $(m-2)\,C$, $3C$ und $(m-3)\,C$ u. s. w. entgegengesetzt sein. Wenn daher m gerade ist, so ist die Klasse $\frac{1}{2}mC$ sich selbst entgegengesetzt und daher ambig; umgekehrt, wenn in $\mathfrak{C}$ ausser K noch eine andere ambige Klasse vorkommt, etwa gC, wird $gC = (m-g)\,C$ und daher $g = m - g = \frac{1}{2}m$ sein. Hieraus folgt, dass, wenn m gerade ist, ausser den beiden Klassen K und $\frac{1}{2}mC$, wenn aber m ungerade ist, ausser der einen Klasse K keine andere ambige Klasse in $\mathfrak{C}$ enthalten sein kann.

IV. Wenn man annimmt, dass die Periode irgend einer in $\mathfrak{C}$ enthaltenen Klasse hC

$$K,\ hC,\ 2hC,\ 3hC,\ \ldots,\ (m'-1)\,hC$$

sei, so ist offenbar $m'h$ das kleinste durch m teilbare Vielfache von h. Wenn daher m und h prim zu einander sind, so ist $m' = m$, und die beiden Perioden werden dieselben Klassen, nur in verschiedener Reihenfolge enthalten; allgemein aber ist, wenn μ den grössten gemeinschaftlichen Teiler von m und h bezeichnet, $m' = \frac{m}{\mu}$. Hieraus geht hervor, dass die Anzahl der in der Periode irgend einer Klasse aus $\mathfrak{C}$ enthaltenen Klassen entweder gleich m oder gleich einem aliquoten Teile von m ist, und zwar werden soviele Klassen in $\mathfrak{C}$ Perioden von m Gliedern haben, als es unter den Zahlen $0, 1, 2, \ldots, m-1$ zu m prime Zahlen giebt, also $\varphi(m)$, wenn man sich der Bezeichnung des Artikels 39 bedient; allgemein aber haben soviel Klassen in $\mathfrak{C}$ Perioden von $\frac{m}{\mu}$ Gliedern, als unter den Zahlen $0, 1, 2 \ldots,$

$m-1$ mit m den grössten gemeinschaftlichen Teiler μ haben, deren Anzahl, wie leicht ersichtlich, $\varphi\left(\frac{m}{\mu}\right)$ ist. Wenn daher $m=n$ oder also das ganze Hauptgeschlecht unter $\mathfrak{C}$ enthalten ist, so giebt es in diesem Geschlecht im Ganzen $\varphi(n)$ Klassen, deren Perioden dasselbe Geschlecht ganz enthalten, und $\varphi(e)$ Klassen, deren Perioden aus e Gliedern bestehen, wo e irgend einen Teiler von n bezeichnet. Dieser Schluss gilt allgemein, wenn es im Hauptgeschlecht irgend eine Klasse giebt, deren Periode aus n Gliedern besteht.

V. Unter derselben Voraussetzung kann das System der Klassen des Hauptgeschlechts nicht zweckmässiger aufgestellt werden, als wenn man irgend eine eine Periode mit n Gliedern besitzende Klasse gewissermassen als Basis nimmt und die Klassen des Hauptgeschlechts in derjenigen Reihenfolge anordnet, in welcher sie in der Periode jener fortschreiten. Wenn dann der Hauptklasse der Index 0, der Klasse, welche als Basis genommen ist, der Index 1 u. s. w. beigelegt wird, so kann man durch blosse Addition der Indices finden, welche Klasse durch Composition irgend welcher Klassen des Hauptgeschlechts hervorgeht. Hier ist ein Beispiel für die Determinante -356, wo wir die Klasse (9, 2, 40) zur Basis genommen haben.

0 (1, 0, 356)	4 (20, 8, 21)	8 (20, −8, 21)
1 (9, 2, 40)	5 (17, 1, 21)	9 (8, 2, 45)
2 (5, 2, 72)	6 (4, 0, 89)	10 (5, −2, 72)
3 (8, −2, 45)	7 (17, −1, 21)	11 (9, −2, 40).

VI. Obwohl es aber sowohl die Analogie mit Abschnitt III als auch die Untersuchung von mehr als 200 negativen Determinanten und von noch weit mehr positiven nichtquadratischen Determinanten höchst wahrscheinlich zu machen scheint, dass jene Voraussetzung für alle Determinanten stattfindet, so würde ein solcher Schluss doch falsch sein und durch eine Fortsetzung der Tafel für die Klasseneinteilungen widerlegt werden. Wir wollen der Kürze wegen diejenigen Determinanten, für welche das ganze Hauptgeschlecht in einer einzigen Periode enthalten sein kann, **reguläre**, die übrigen aber, für welche dieses nicht möglich ist, **irreguläre Determinanten** nennen. Diesen Gegenstand, welcher zu den verstecktesten Geheimnissen der höheren Arithmetik zu gehören und den schwierigsten Untersuchungen Raum zu gewähren scheint, können wir hier nur durch wenige Bemerkungen illustrieren, denen wir die folgende allgemeine Bemerkung vorausschicken.

VII. Wenn im Hauptgeschlechte die Klassen C, C' vorkommen, deren Perioden aus m, m' Klassen bestehen und M die kleinste durch m und m' teilbare Zahl ist, so giebt es in demselben Geschlechte auch Klassen, deren Perioden M Glieder enthalten. Zerlegt man M in zwei zu einander prime

Factoren r, r', von denen der eine (r) in m, der andere (r') in m' aufgeht (Artikel 73), so hat die Klasse $\frac{m}{r}C + \frac{m'}{r'}C' = C''$ die verlangte Eigenschaft. Denn nehmen wir an, dass die Periode der Klasse C'' aus g Gliedern bestehe, so ist

$$K = grC'' = gmC + \frac{grm'}{r'}C' = K + \frac{grm'}{r'}C' = \frac{grm'}{r'}C';$$

demnach muss $\frac{grm'}{r'}$ durch m' oder gr durch r' und somit auch g durch r' teilbar sein. In ganz ähnlicher Weise findet man, dass g durch r teilbar ist, so dass auch g durch $rr' = M$ teilbar ist. Da aber offenbar $MC'' = K$ ist, so wird auch M durch g teilbar und daher notwendig $M = g$ sein. Hieraus folgt leicht, dass die grösste Anzahl der in irgend einer Periode (für eine gegebene Determinante) enthaltenen Klassen durch die Anzahl der Klassen in jeder andern Periode (einer Klasse aus demselben Hauptgeschlechte) teilbar ist. Gleichzeitig kann ebendaraus eine Methode abgeleitet werden, eine solche Klasse, deren Periode möglichst gross ist (und daher für eine reguläre Determinante das ganze Hauptgeschlecht umfasst), zu ermitteln, eine Methode, die der Methode in den Artikeln 73, 74 völlig analog ist, obwohl in der Praxis die Arbeit durch mehrere Kunstgriffe zusammenzogen werden kann. Der Quotient der Division der Zahl n durch die Klassenanzahl in der grössten Periode, welcher bei regulären Determinanten gleich 1 ist, wird für irreguläre Determinanten stets eine ganze Zahl, die grösser als 1 ist, und ist für solche ganz besonders geeignet, die verschiedenen Arten der Irregularität auszudrücken, und kann daher **Irregularitätsexponent** genannt werden.

VIII. Bisher hat man keine allgemeine Regel, durch welche man die regulären Determinanten von vornherein von den irregulären unterscheiden könnte, besonders weil sich unter den letzteren sowohl prime als auch zusammengesetzte Zahlen vorfinden; es möge daher genügen, hier einige specielle Bemerkungen anzuknüpfen. Wenn in dem Hauptgeschlechte mehr als zwei ambige Klassen enthalten sind, so ist die Determinante sicher irregulär und der Irregularitätsexponent gerade; wenn aber nur eine oder zwei ambige Klassen in jenem Geschlechte vorhanden sind, so ist die Determinante entweder regulär oder wenigstens der Irregularitätsexponent ungerade. Alle negativen Determinanten von der Form $-(216k + 27)$, die eine -27 allein ausgenommen, sind irregulär und der Irregularitätsexponent ist durch 3 teilbar; dasselbe gilt von den negativen Determinanten von der Form $-(1000k + 75)$ und $-(1000k + 675)$, die eine -75 allein ausgenommen, und von unzählig vielen andern. Ist der Irregularitätsexponent eine Primzahl p oder wenigstens durch p teilbar, so ist n durch p^2 teilbar, woraus folgt, dass, wenn n keinen quadratischen Teiler enthält, die Determinante sicher regulär ist. Nur für positive quadratische Determinanten e^2

kann man immer von vornherein entscheiden, ob sie regulär oder irregulär sind; jenes findet nämlich statt, wenn e entweder 1 oder 2 oder eine ungerade Primzahl oder die Potenz einer ungeraden Primzahl ist; dieses in allen übrigen Fällen. Für negative Determinanten werden die irregulären immer häufiger, je grösser die Determinanten sind; so finden sich z. B. in dem ganzen ersten Tausend dreizehn irreguläre, nämlich (mit Weglassung des negativen Vorzeichens) 576, 580, 820, 884, 900, deren Irregularitätsexponent 2, und 243, 307, 339, 459, 675, 755, 891, 974, deren Irregularitätsexponent 3 ist; in dem zweiten Tausend finden sich 13, deren Irregularitätsexponent 2, und 15, deren Irregularitätsexponent 3 ist;*) im zehnten Tausend finden sich 31 mit dem Irregularitätsexponenten 2 und 32 mit dem Irregularitätsexponenten 3. Ob unterhalb — 10000 Determinanten mit einem Irregularitätsexponenten, der grösser als 3 ist, vorkommen, kann ich noch nicht entscheiden; jenseits dieser Grenze können sich irgend welche gegebene Exponenten ergeben. Dass sich die Häufigkeit der irregulären negativen Determinanten zur Häufigkeit der regulären mit wachsenden Determinanten mehr und mehr einem constanten Verhältnis nähert, ist höchst wahrscheinlich, und würde die Bestimmung dieses Verhältnisses eine der Bemühungen der Geometer würdige Aufgabe sein. — Für positive nichtquadratische Determinanten sind die irregulären viel seltener; solche, deren Irregularitätsexponent gerade ist, giebt es jedenfalls unendlich viele (z. B. 3026, für welche derselbe gleich 2 ist); auch erscheint es nicht zweifelhaft, dass solche existieren, deren Irregularitätsexponent ungerade ist, obwohl wir gestehen müssen, dass uns eine solche bisher nicht aufgestossen ist.

IX. Über die bequemste Anordnung des Systems der Klassen, welche für eine irreguläre Determinante im Hauptgeschlechte enthalten sind, können wir hier der Kürze wegen nicht handeln; wir bemerken nur, da eine einzige Basis hierzu nicht ausreicht, dass man hier zwei oder sogar noch mehrere Klassen annehmen muss, durch deren Multiplikation und Composition alle andern entstehen. Hierdurch ergeben sich doppelte und vielfache Indices, die ungefähr denselben Nutzen gewähren, wie die einfachen bei den regulären Determinanten. Diesen Gegenstand werden wir jedoch bei anderer Gelegenheit ausführlicher behandeln.

X. Endlich bemerken wir, dass, da alle in diesem und dem vorigen Artikel betrachteten Eigenschaften hauptsächlich von der Zahl n abhängen, welche etwas Ähnliches ist wie die Zahl $p-1$ im Abschnitt III, diese Zahl die grösste Beachtung verdient, und wäre es somit auf das innigste zu wünschen, dass zwischen ihr und der Determinante, zu der sie gehört, ein allgemeiner Zusammenhang entdeckt würde. An dieser sehr wichtigen Sache glauben wir um so weniger verzweifeln zu dürfen, als es bereits gelungen ist, den mittleren Wert des Products aus n und der Anzahl der

*) Vgl. die Zusätze am Schlusse der *Disquisitiones*.

Geschlechter (welche von vornherein bestimmt werden kann) wenigstens für negative Determinanten durch eine analytische Formel darzustellen (Artikel 302).*)

307.

Die Untersuchungen der vorigen Artikel umfassen nur die Klassen des Hauptgeschlechts und reichen daher sowohl für positive Determinanten, in denen es überhaupt nur ein Geschlecht giebt, als auch für negative Determinanten aus, für welche es nur ein positives Geschlecht giebt, wenn wir auf das negative Geschlecht keine Rücksicht nehmen wollen. Wir haben daher nur noch in Bezug auf die übrigen (eigentlich primitiven) Geschlechter Einiges hinzuzufügen.

I. Wenn es in dem Geschlechte G', welches vom Hauptgeschlechte G (mit derselben Determinante) verschieden ist, irgend eine ambige Klasse giebt, so giebt es in ihm ebensoviele wie in G. Es mögen in G die ambigen Klassen L, M, N, ... (unter denen sich auch die Hauptklasse K befindet), in G' aber die ambigen Klassen L', M', N', ... sein, und es möge die Gesamtheit jener mit A, die Gesamtheit dieser mit A' bezeichnet werden. Da offenbar sämtliche Klassen $L+L'$, $M+L'$, $N+L'$, ... ambig und verschieden sind und zu G' gehören, also unter A' enthalten sein müssen, so kann die Anzahl der Klassen in A' sicher nicht kleiner sein als in A; da ebenso $L'+L'$, $M'+L'$, $N'+L'$, ... von einander verschieden und ambig sind und zu G gehören, also unter A enthalten sind, so kann die Anzahl der Klassen in A nicht kleiner sein als in A'. Daher sind die Anzahlen der Klassen in A und A' notwendig einander gleich.

II. Da die Anzahl aller ambigen Klassen der Anzahl der Geschlechter gleich ist (Artikel 261, 287 III), so darf offenbar, wenn es in G nur eine ambige Klasse giebt, in jedem Geschlechte nur eine ambige Klasse enthalten sein; wenn aber in G zwei ambige Klassen existieren, so muss es in der Hälfte aller Geschlechter je zwei, in den übrigen gar keine geben; und wenn in G mehrere, etwa a**), ambige Klassen enthalten sind, so wird der a^{te} Teil sämtlicher Geschlechter je a ambige Klassen, die übrigen aber gar keine solchen enthalten.

III. Es seien für den Fall, wo G zwei ambige Klassen enthält, $G, G', G'', \ldots$ diejenigen Geschlechter, welche je zwei und $H, H', H'', \ldots$ diejenigen, welche keine ambigen Klassen enthalten, und man bezeichne die Gesamtheit jener mit $\mathfrak{G}$, die Gesamtheit dieser mit $\mathfrak{H}$. Da durch Composition zweier ambigen Klassen immer eine ambige Klasse entsteht (Artikel 249), so ist leicht ersichtlich, dass durch Composition zweier Geschlechter aus $\mathfrak{G}$ immer ein Geschlecht aus $\mathfrak{G}$ hervorgeht. Hieraus folgt ferner, dass durch Composition eines Geschlechtes aus $\mathfrak{G}$ mit einem

*) Vgl. die Zusätze am Schlusse der *Disquisitiones*.

**) Dies kann nur für irreguläre Determinanten stattfinden, und es ist a immer eine Potenz von 2.

Geschlechte aus $\mathfrak{H}$ ein Geschlecht aus $\mathfrak{H}$ entsteht. Denn wenn z. B. $G' + H$ nicht zu $\mathfrak{H}$ sondern zu $\mathfrak{G}$ gehörte, so würde auch $G' + H + G'$ zu $\mathfrak{G}$ gehören müssen, was absurd ist, da $G' + G' = G$ und daher $G' + H + G' = H$ ist. Endlich folgert man leicht, dass die Geschlechter $G + H$, $G' + H$, $G'' + H, \ldots$ zusammen mit $H + H$, $H' + H$, $H'' + H, \ldots$ sämtlich verschieden und daher mit $\mathfrak{G}$ und $\mathfrak{H}$ zusammengenommen identisch sind; nach dem soeben Bewiesenen gehören aber die Geschlechter $G + H$, $G' + H$, $G'' + H, \ldots$ sämtlich zu $\mathfrak{H}$ und erschöpfen somit diesen Complex, daher werden die übrigen $H + H$, $H' + H$, $H'' + H, \ldots$ sämtlich zu $\mathfrak{G}$ gehören, d. h. durch Composition zweier Geschlechter aus $\mathfrak{H}$ entsteht immer ein Geschlecht aus $\mathfrak{G}$.

IV. Ist E eine Klasse des vom Hauptgeschlecht G verschiedenen Geschlechts V, so werden offenbar $2E$, $4E$, $6E, \ldots$ sämtlich zu G, dagegen $3E$, $5E$, $7E, \ldots$ sämtlich zu V gehören. Wenn daher die Periode der Klasse $2E$ aus m Gliedern besteht, so wird offenbar in der Reihe E, $2E$, $3E, \ldots$ die Klasse $2mE$ und keine frühere mit K identisch sein, oder die Periode der Klasse E wird aus $2m$ Gliedern bestehen. Hiernach ist die Anzahl der Glieder in der Periode einer jeden Klasse, welche zu einem andern Geschlechte als dem Hauptgeschlechte gehört, entweder $2n$ oder ein aliquoter Teil von $2n$, wenn n die Anzahl der Klassen in den einzelnen Geschlechtern bezeichnet.

V. Es sei C eine gegebene Klasse des Hauptgeschlechts G, E eine Klasse des Geschlechts V, durch deren Duplikation C entsteht (eine solche giebt es stets, Artikel 286), und es seien ferner K, K', $K'', \ldots$ sämtliche ambigen (eigentlich primitiven mit derselben Determinante) Klassen. Dann sind sämtliche Klassen, durch deren Duplikation C entsteht, die folgenden: $E (= E + K)$, $E + K'$, $E + K'', \ldots$, deren Complex durch Ω dargestellt werden möge; die Anzahl dieser Klassen ist gleich der Anzahl der ambigen Klassen oder gleich der Anzahl der Geschlechter. Es ist klar, dass von den Klassen in Ω soviel zum Geschlechte V gehören, als es in G ambige Klassen giebt; bezeichnet man daher die Anzahl dieser mit a, so giebt es offenbar in jedem Geschlechte entweder a Klassen aus Ω oder gar keine. Hieraus folgt leicht, dass, wenn $a = 1$ ist, in jedem Geschlechte eine Klasse aus Ω enthalten ist; dass ferner, wenn $a = 2$ ist, die Hälfte aller Geschlechter je zwei Klassen aus Ω, die übrigen aber gar keine enthalten, und dass die erstere Hälfte entweder ganz mit $\mathfrak{G}$, die letztere ganz mit $\mathfrak{H}$, oder diese mit $\mathfrak{G}$ und jene mit $\mathfrak{H}$ zusammenfällt (in derselben Bedeutung wie oben in III). — Ist a noch grösser, so wird der a^{te} Teil aller Geschlechter die Klassen Ω enthalten (und zwar jedes einzelne a Klassen).

VI. Nehmen wir nun an, dass C eine solche Klasse sei, deren Periode aus n Gliedern besteht, so sieht man leicht, dass in dem Falle, wo $a = 2$ und daher n gerade ist, keine Klasse aus Ω zu G gehören kann (denn dann würde eine solche Klasse in der Periode von C enthalten sein; wenn dieselbe also gleich rC oder $2rC = C$ wäre, so würde $2r \equiv 1 \pmod{n}$ sein,

was absurd ist); somit müssen, da G zu $\mathfrak{G}$ gehört, notwendig alle Klassen Ω unter die Geschlechter $\mathfrak{H}$ verteilt sein. Hieraus folgt, da es (für eine reguläre Determinante) in G im Ganzen $\varphi(n)$, Perioden von n Gliedern besitzende Klassen giebt, dass sich für den Fall, wo $a = 2$ ist, in jedem Geschlechte $\mathfrak{H}$ im Ganzen $2\varphi(n)$ Klassen vorfinden, deren Perioden $2n$ Glieder und daher sowohl ihr eigenes Geschlecht als auch das Hauptgeschlecht umfassen; ist dagegen $a = 1$, so giebt es in jedem vom Hauptgeschlechte verschiedenen Geschlechte $\varphi(n)$ derartige Klassen.

VII. Auf diese Bemerkungen gründen wir die folgende Methode, das System aller eigentlich primitiven Klassen für jede gegebene reguläre (denn die irregulären lassen wir gänzlich bei Seite) Determinante möglichst zweckmässig aufzustellen. Man wähle nach Belieben eine Klasse E aus, deren Periode $2n$ Glieder und daher sowohl ihr eigenes Geschlecht, welches V sei, als auch das Hauptgeschlecht enthält; die Klassen dieser beiden Geschlechter ordne man so an, wie sie in jener Periode fortschreiten. Auf diese Weise ist die Sache bereits erledigt, wenn es keine Geschlechter weiter als diese beiden giebt, oder es nicht nötig erscheint, die übrigen hinzuzunehmen (z. B. bei einer solchen negativen Determinante, bei welcher es nur zwei positive Geschlechter giebt). Wenn aber vier oder mehr Geschlechter aufzustellen sind, so behandle man die übrigen in folgender Weise: Ist V' irgend eins von den übrigen und $V + V' = V''$, so giebt es in V' und V'' zwei ambige Klassen (nämlich entweder in jeder der beiden eine oder in der einen zwei, in der andern gar keine); aus diesen wähle man eine nach Belieben aus, so folgt leicht, dass, wenn A mit den einzelnen Klassen in G und V zusammengesetzt wird, $2n$ verschiedene zu V' und V'' gehörige und daher diese Geschlechter völlig erschöpfende Klassen entstehen; daher können auch diese Geschlechter geordnet werden. — Wenn ausser diesen vier Geschlechtern noch andere übrig sind, so sei V''' eins von den übrigen, und ferner seien V'''', V''''', V'''''' diejenigen Geschlechter, welche durch Composition des Geschlechts V''' mit V, V' und V'' entstehen. Diese vier Geschlechter V''', V'''', ..., V'''''' enthalten vier ambige Klassen, und es ist klar, dass, wenn von diesen eine A' ausgewählt und mit den einzelnen Klassen in G, V, V', V'' zusammengesetzt wird, alle Klassen in V''', ..., V'''''' hervorgehen. — Sind noch mehr Geschlechter übrig, so fahre man in derselben Weise fort, bis sie sämtlich erschöpft sind. Offenbar wird man, wenn die Anzahl aller aufzustellenden Geschlechter 2^μ ist, im Ganzen $2^{\mu-1}$ ambige Klassen nötig haben, und jede Klasse dieser Geschlechter wird hervorgebracht werden können entweder durch Multiplikation der Klasse E oder durch Composition einer durch eine solche Multiplikation entstandenen Klasse mit einer oder mehreren ambigen. Wir geben hier zwei **Beispiele**, durch welche diese Regeln erläutert werden sollen; mehr können wir hier über den Nutzen derartiger Constructionen oder über die Kunstgriffe, durch welche die Arbeit erleichtert werden kann, nicht hinzufügen.

I. Determinante — 161.

Vier positive Geschlechter; in jedem einzelnen vier Klassen.

G	V
1,4; $R7$; $R23$	3,4; $N7$; $R23$
$(1, \ 0, \ 161) = K$	$(3, \ 1, \ 54) = E$
$(9, \ 1, \ 18) = 2E$	$(6, \ -1, \ 27) = 3E$
$(2, \ 1, \ 81) = 4E$	$(6, \ 1, \ 27) = 5E$
$(9, \ -1, \ 18) = 6E$	$(3, \ -1, \ 54) = 7E$

V'	V''
3,4; $R7$; $N23$	1,4; $N7$; $N23$
$(7, \ 0, \ 23) = A$	$(10, \ 3, \ 17) = A + E$
$(11, \ -2, \ 15) = A + 2E$	$(5, \ 2, \ 33) = A + 3E$
$(14, \ 7, \ 15) = A + 4E$	$(5, \ -2, \ 33) = A + 5E$
$(11, \ 2, \ 15) = A + 6E$	$(10, \ -3, \ 17) = A + 7E.$

II. Determinante — 546.

Acht positive Geschlechter; in jedem einzelnen drei Klassen.

G	V
1 u. 3,8; $R3$; $R7$; $R13$	3 u. 7,8; $N3$; $N7$; $N13$
$(1, \ 0, \ 546) = K$	$(5, \ 2, \ 110) = E$
$(22, \ -2, \ 25) = 2E$	$(21, \ 0, \ 26) = 3E$
$(12, \ 2, \ 25) = 4E$	$(5, \ -2, \ 110) = 5E$

V'	V''
1 u. 3,8; $N3$; $R7$; $N13$	5 u. 7,8; $R3$; $N7$; $R13$
$(2, \ 0, \ 273) = A$	$(10, \ 2, \ 55) = A + E$
$(11, \ -2, \ 50) = A + 2E$	$(13, \ 0, \ 42) = A + 3E$
$(11, \ 2, \ 50) = A + 4E$	$(10, \ -2, \ 55) = A + 5E$

V'''	V''''
1 u. 3,8; $N3$; $N7$; $R13$	5 u. 7,8; $R3$; $R7$; $N13$
$(3, \ 0, \ 182) = A'$	$(15, \ -3, \ 37) = A' + E$
$(17, \ 7, \ 35) = A' + 2E$	$(7, \ 0, \ 78) = A' + 3E$
$(17, \ -7, \ 35) = A' + 4E$	$(15, \ 3, \ 37) = A' + 5E$

V'''''	V''''''
1 u. 3,8; $R3$; $N7$; $N13$	5 u. 7,8; $N3$; $R7$; $R13$
$(6, \ 0, \ 91) = A + A'$	$(23, \ 11, \ 29) = A + A' + E$
$(19, \ 9, \ 33) = A + A' + 2E$	$(14, \ 0, \ 39) = A + A' + 3E$
$(19, \ -9, \ 33) = A + A' + 4E$	$(23, \ -11, \ 29) = A + A' + 5E.$

Sechster Abschnitt.

Verschiedene Anwendungen der vorhergehenden Untersuchungen.



308.

Wie fruchtbar die höhere Arithmetik an Wahrheiten ist, welche auch in andern Teilen der Mathematik Nutzen gewähren, haben wir bereits an mehreren Stellen vorübergehend berührt; wir haben es aber für nicht unnützlich gehalten, gewisse Anwendungen, welche eine ausführlichere Auseinandersetzung verdienen, für sich zu behandeln, nicht sowohl um diesen Gegenstand, mit dem man leicht mehrere Bände füllen könnte, zu erschöpfen, als vielmehr ihn durch einige Proben in ein helleres Licht zu setzen. Im gegenwärtigen Abschnitte werden wir zuerst von der Zerlegung der Brüche in einfachere, sodann von der Verwandlung der gemeinen Brüche in Decimalbrüche handeln; darauf werden wir eine neue Ausschliessungsmethode, welche zur Auflösung der unbestimmten Gleichungen zweiten Grades dient, auseinandersetzen; endlich werden wir neue einfache Methoden angeben, um die Primzahlen von den zusammengesetzten zu unterscheiden und die Factoren der letzteren zu ermitteln. Im folgenden Abschnitte aber werden wir die allgemeine Theorie einer besonderen in der gesamten Analysis sehr häufig angewandten Art von Functionen, soweit sie mit der höheren Arithmetik in innigstem Zusammenhange steht, begründen und insbesondere die Theorie der Kreisteilung, von der bisher nur die ersten Elemente bekannt waren, durch neue Zuthaten zu erweitern suchen.

Zerlegung der Brüche in einfachere.

309.

Aufgabe. Den Bruch $\frac{m}{n}$, dessen Nenner das Product aus zwei zu einander primen Zahlen a, b ist, in zwei andere zu zerlegen, deren Nenner a und b sind.

Auflösung. Sind die gesuchten Brüche $\frac{x}{a}$, $\frac{y}{b}$, so muss $bx + ay = m$ werden; demnach ist x die Wurzel der Congruenz $bx \equiv m$ (mod. a), die man nach Abschnitt II finden kann; y aber wird gleich $\frac{m - bx}{a}$.

Übrigens ist bekannt, dass die Congruenz $bx \equiv m$ unendlich viele, aber nach dem Modul a congruente Wurzeln besitzt, dass es aber nur eine einzige positive Wurzel, welche kleiner als a ist, giebt; ferner kann es aber auch geschehen, dass y negativ wird. Es wird kaum nötig sein, darauf hinzuweisen, dass y auch durch die Congruenz $ay \equiv m$ (mod. b) und x durch die Gleichung $x = \frac{m - ay}{b}$ gefunden werden kann. — Ist z. B. der Bruch $\frac{58}{77}$ gegeben, so ist 4 der Wert des Ausdrucks $\frac{58}{11}$ (mod. 7), und somit zerfällt $\frac{58}{77}$ in $\frac{4}{7} + \frac{2}{11}$.

310.

Ist ein Bruch $\frac{m}{n}$ gegeben, dessen Nenner n das Product aus beliebig vielen zu einander primen Zahlen $a, b, c, d, \ldots$ ist, so kann derselbe nach dem vorigen Artikel zunächst in zwei zerlegt werden, deren Nenner a und $bcd\ldots$ sind; der zweite wiederum in zwei mit den Nennern b und $cd\ldots$; der letztere wiederum in zwei u. s. f., bis endlich der gegebene Bruch auf die Form gebracht ist:

$$\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \frac{\delta}{d} + \cdots$$

Die Zähler $\alpha, \beta, \gamma, \delta \ldots$ kann man offenbar positiv und kleiner als ihre Nenner annehmen, mit Ausnahme des letzten, welcher, nachdem die übrigen bestimmt sind, nicht weiter willkürlich ist und auch negativ und grösser als der Nenner werden kann (wofern wir nicht $m < n$ voraussetzen). Dann wird es meistens zweckmässig sein, ihn auf die Form $\frac{\varepsilon}{e} \mp k$ zu bringen, so dass ε eine positive Zahl und kleiner als e, k aber eine ganze Zahl ist. Endlich ist klar, dass $a, b, c, \ldots$ so angenommen werden können, dass sie entweder Primzahlen oder Potenzen von Primzahlen sind.

Beispiel. Der Bruch $\frac{391}{924}$, dessen Nenner gleich $4 \cdot 3 \cdot 7 \cdot 11$ ist, wird auf diese Weise zerlegt in $\frac{1}{4} + \frac{40}{231}$; $\frac{40}{231}$ in $\frac{2}{3} - \frac{38}{77}$; $-\frac{38}{77}$ in $\frac{1}{7} - \frac{7}{11}$, so dass, wenn man $\frac{4}{11} - 1$ für $-\frac{7}{11}$ schreibt, $\frac{391}{924} = \frac{1}{4} + \frac{2}{3} + \frac{1}{7} + \frac{4}{11} - 1$ wird.

311.

Der Bruch $\frac{m}{n}$ lässt sich nur auf eine einzige Weise auf die Form $\frac{\alpha}{a} + \frac{\beta}{b} + \cdots \mp k$ derart bringen, dass α, β, ... positiv und kleiner als a, b, ... respective sind; denn nimmt man an, dass

$$\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \cdots \mp k = \frac{\alpha'}{a} + \frac{\beta'}{b} + \frac{\gamma'}{c} + \cdots \mp k'$$

sei, und dass auch α', β', ... positive Zahlen und bezüglich kleiner als a, b, ... seien, so muss notwendig $\alpha = \alpha'$, $\beta = \beta'$, $\gamma = \gamma'$, ..., $k = k'$ sein. Multipliciert man nämlich mit $n = abc \ldots$, so wird offenbar $m \equiv \alpha bcd \ldots \equiv \alpha' bcd \ldots \pmod{a}$ und daher, weil $bcd \ldots$ zu a prim ist, notwendig $\alpha \equiv \alpha'$ und somit $\alpha = \alpha'$, und ebenso $\beta = \beta'$, u. s. w., woraus von selbst $k = k'$ folgt. Da es nun vollständig willkürlich ist, für welchen Nenner der Zähler zuerst berechnet wird, so ist ersichtlich, dass alle Zähler so wie α im vorigen Artikel gefunden werden können, nämlich β durch die Congruenz $\beta acd \ldots \equiv m \pmod{b}$, γ durch $\gamma abd \ldots \equiv m \pmod{c}$, u. s. w. Die Summe aller so gefundenen Brüche ist entweder gleich dem gegebenen Bruche $\frac{m}{n}$ oder der Unterschied ist eine ganze Zahl k, so dass wir auf diese Weise zugleich eine Bestätigung der Rechnung erhalten. So ergeben z. B. im Beispiel des vorigen Artikels die Werte der Ausdrücke $\frac{391}{231} \pmod{4}$, $\frac{391}{308} \pmod{3}$, $\frac{391}{132} \pmod{7}$, $\frac{391}{84} \pmod{11}$ sogleich die den Nennern 4, 3, 7, 11 entsprechenden Zähler 1, 2, 1, 4, und man findet, dass die Summe dieser Brüche den gegebenen Bruch um eine Einheit übersteigt.

Verwandlung der gemeinen Brüche in Decimalbrüche.

312.

Erklärung. Wenn ein gemeiner Bruch in einen Decimalbruch verwandelt wird, so nennen wir die Reihe der Decimalzahlen*) (mit Ausschluss der ganzen Zahl, wenn eine vorhanden ist), mag dieselbe endlich sein oder ins Unendliche gehen, die **Mantisse** des Bruches, indem wir den Ausdruck, der sonst nur bei den Logarithmen gebräuchlich ist, in einer weiteren Bedeutung nehmen. So ist z. B. die Mantisse des Bruches $\frac{1}{8}$ gleich 125, die Mantisse des Bruches $\frac{35}{16}$ gleich 1875, die Mantisse des Bruches $\frac{2}{37}$ gleich 054054 .... *in inf.*

*) Der Kürze halber beschränken wir die folgende Untersuchung auf das gemeine decadische System, da sie sich leicht auf jedes beliebige System ausdehnen lässt.

Aus dieser Erklärung geht sogleich hervor, dass Brüche mit demselben Nenner $\frac{l}{n}$, $\frac{m}{n}$ dieselben oder verschiedene Mantissen haben, je nachdem die Zähler l, m nach n congruent oder incongruent sind. Eine endliche Mantisse wird nicht geändert, wenn man rechts beliebig viele Nullen ansetzt. Die Mantisse des Bruches $\frac{10m}{n}$ erhält man, wenn man von der Mantisse des Bruches $\frac{m}{n}$ die erste Ziffer abschneidet, und allgemein, die Mantisse des Bruches $\frac{10^\nu m}{n}$ findet man, wenn man von der Mantisse des Bruches $\frac{m}{n}$ die ν ersten Ziffern abschneidet. Die Mantisse des Bruches $\frac{1}{n}$ beginnt sogleich mit einer geltenden (d. h. von Null verschiedenen) Ziffer, wenn n nicht grösser als 10 ist; ist aber $n > 10$ und keiner Potenz von 10 gleich, und die Anzahl der Ziffern, aus denen sie besteht, gleich k, so sind die $k-1$ ersten Ziffern der Mantisse Nullen und erst die folgende k^{te} ist eine geltende Ziffer. Hieraus folgt leicht, dass, wenn $\frac{l}{n}$, $\frac{m}{n}$ verschiedene Mantissen haben (d. h. wenn l, m nach n incongruent sind), diese sicher nicht in den ersten k Ziffern übereinstimmen können, sondern wenigstens in der k^{ten} von einander abweichen müssen.

313.

Aufgabe. Wenn der Nenner des Bruches $\frac{m}{n}$ und die ersten k Ziffern seiner Mantisse gegeben sind, so soll man den Zähler m finden, den wir kleiner als n voraussetzen.

Auflösung. Man betrachte jene k Ziffern als eine ganze Zahl, multipliciere dieselbe mit n und dividiere das Product durch 10^k (oder schneide die k letzten Ziffern ab). Ist der Quotient eine ganze Zahl (oder sind die abgeschnittenen Ziffern Nullen), so ist derselbe selbst der gesuchte Zähler und die gegebene Mantisse vollständig; wenn nicht, so ist der gesuchte Zähler die nächsthöhere ganze Zahl oder jener um eine Einheit vermehrte Quotient, nachdem die folgenden Decimalstellen abgeschnitten worden sind. Der Grund dieser Regel ist aus unsern Bemerkungen am Schlusse des vorigen Artikels so leicht ersichtlich, dass es einer weiteren Auseinandersetzung nicht bedarf.

Beispiel. Wenn man weiss, dass die beiden ersten Ziffern der Mantisse eines Bruches, dessen Nenner 23 ist, 69 seien, so hat man das Product $23 \cdot 69 = 1587$; wirft man hiervon die beiden letzten Ziffern weg und addiert 1, so ergiebt sich der gesuchte Zähler gleich 16.

314.

Wir beginnen mit der Betrachtung solcher Brüche, deren Nenner Primzahlen oder Potenzen von Primzahlen sind, und werden nachher zeigen, wie man die übrigen auf diese zurückführen kann. Zunächst bemerken wir sogleich, dass die Mantisse des Bruches $\frac{a}{p^\mu}$ (von dessen Zähler a wir stets voraussetzen, dass er durch die Primzahl p nicht teilbar sei) endlich ist und aus μ Ziffern besteht, wenn $p = 2$ oder $p = 5$ ist; im ersteren Falle ist diese Mantisse, als ganze Zahl betrachtet, gleich $5^\mu a$, im letzteren gleich $2^\mu a$. Dies ist so klar, dass es einer Auseinandersetzung nicht bedarf.

Ist aber p eine andere Primzahl, so wird $10^r a$ durch p^μ niemals teilbar sein, wie gross man auch r annehmen möge, woraus unmittelbar folgt, dass die Mantisse des Bruches $F = \frac{a}{p^\mu}$ notwendig ins Unendliche fortgeht. Nehmen wir an, 10^e sei die niedrigste Potenz von 10, welche der Einheit nach dem Modul p^μ congruent ist (vgl. Abschnitt III, wo wir gezeigt haben, dass e entweder gleich der Zahl $(p-1)\,p^{\mu-1}$ oder ein aliquoter Teil derselben ist), so erkennt man leicht, dass auch $10^e a$ in der Reihe $10a$, $100a$, $1000a, \ldots$ die erste Zahl ist, welche a nach demselben Modul congruent ist. Da nun nach Artikel 312 die Mantissen der Brüche $\frac{10a}{p^\mu}$, $\frac{100a}{p^\mu}, \ldots, \frac{10^e a}{p^\mu}$ entstehen, indem man von der Mantisse des Bruches F die erste Ziffer oder die beiden, u. s. w., e ersten Ziffern respective fortlässt, so ist klar, dass in dieser Mantisse nach den e ersten Ziffern und nicht eher dieselben Ziffern sich nochmals wiederholen. Diese ersten e Ziffern, aus deren unendlich oftmaliger Wiederholung die Mantisse gebildet ist, können wir die **Periode** dieser Mantisse oder des Bruches F nennen, und es ist ersichtlich, dass die Grösse der Periode oder die Anzahl der Ziffern, aus denen sie besteht, und welche gleich e ist, vom Zähler a vollständig unabhängig ist und nur allein durch den Nenner bestimmt wird. So ist z. B. die Periode des Bruches $\frac{1}{11}$ gleich 09, die Periode des Bruches $\frac{3}{7}$ gleich 428571.*)

315.

Sobald man daher die Periode irgend eines Bruches hat, kann die Mantisse auf beliebig viele Stellen fortgesetzt werden. Ferner ergiebt sich, dass, wenn $b \equiv 10^\lambda a \pmod{p^\mu}$ ist, die Periode des Bruches $\frac{b}{p^\mu}$ entsteht,

*) Robertson deutet den Anfang und das Ende der Periode durch zwei über die erste und letzte Ziffer derselben gesetzte Punkte an *(Theory of circulating fractions, Phil. Trans., 1769, p. 207)*, was wir hier nicht für nötig halten.

wenn man die ersten λ Ziffern des Bruches F (wenn wir, was erlaubt ist, $\lambda < e$ annehmen) hinter die übrigen $e - \lambda$ schreibt, und dass man somit zugleich mit der Periode des Bruches F die Perioden sämtlicher Brüche hat, deren Zähler den Zahlen $10a$, $100a$, $1000a$, ... nach dem Nenner p^μ congruent sind. So wird z. B., da $6 \equiv 3 \cdot 10^2$ (mod. 7) ist, die Periode des Bruches $\frac{6}{7}$ sofort aus der Periode des Bruches $\frac{3}{7}$ gleich 857142 gefunden.

So oft daher für den Modul p^μ die Zahl 10 primitive Wurzel ist (Artikel 57, 89), lässt sich aus der Periode des Bruches $\frac{1}{p^\mu}$ sofort die Periode jedes andern Bruches $\frac{m}{p^\mu}$ (dessen Zähler m durch p nicht teilbar ist) ableiten, indem man soviel Stellen von jener links abschneidet und rechts wieder ansetzt, als der Index von m Einheiten besitzt, wenn 10 als Basis genommen wird. Hieraus ist ersichtlich, warum in diesem Falle die Zahl 10 in der Tafel I stets als Basis genommen ist (Artikel 72).

Wenn dagegen 10 keine primitive Wurzel ist, so können aus der Periode des Bruches $\frac{1}{p^\mu}$ die Perioden nur von denjenigen Brüchen abgeleitet werden, deren Zähler irgend einer Potenz von 10 nach dem Modul p^μ congruent sind. Es sei 10^e die niedrigste Potenz von 10, welche der Einheit nach dem Modul p^μ congruent ist, ferner $(p-1)p^{\mu-1} = ef$ und eine solche primitive Wurzel r zur Basis genommen, dass der Index der Zahl 10 gleich f wird (Artikel 71). In diesem System haben somit die Zähler der Brüche, deren Perioden aus der Periode des Bruches $\frac{1}{p^\mu}$ abgeleitet werden können, die Indices $f, 2f, 3f, \ldots, ef-f$; analog können aus der Periode des Bruches $\frac{r}{p^\mu}$ die Perioden der Brüche, deren Zähler $10r$, $100r$, $1000r$, ... den Indices $f+1$, $2f+1$, $3f+1$, ... entsprechen, gefunden werden; aus der Periode des Bruches mit dem Zähler r^2 (dessen Index 2 ist) ergeben sich die Perioden der Brüche mit Zählern, deren Indices $f+2$, $2f+2$, $3f+2$, ... sind, und allgemein lassen sich aus der Periode des Bruches mit dem Zähler r^i die Perioden der Brüche mit Zählern, deren Indices $f+i$, $2f+i$, $3f+i$, ... sind, herleiten. Hieraus schliesst man leicht, dass, wenn man nur die Perioden der Brüche mit den Zählern $1, r, r^2, r^3, \ldots, r^{f-1}$ hat, alle übrigen daraus durch blosse Transposition nach folgender **Regel** abgeleitet werden können:

Es sei der Index des Zählers m eines gegebenen Bruches $\frac{m}{p^\mu}$ in dem System, in welchem r als Basis genommen ist, gleich i (welche Zahl wir kleiner als $(p-1)p^{\mu-1}$ annehmen); es werde (durch Division mit f) $i = \alpha f + \beta$ gesetzt, so dass α, β ganze positive Zahlen (oder auch 0) sind

und $\beta < f$ ist. Ist dies geschehen, so ergiebt sich die Periode des Bruches $\frac{m}{p^\mu}$ aus der Periode des Bruches, dessen Zähler r^β (und daher 1, wenn $\beta = 0$) ist, wenn man die α ersten Ziffern hinter die übrigen setzt (und somit diese Periode selbst beibehält, wenn $\alpha = 0$ ist). Dies wird hinreichend erklären, warum wir bei der Aufstellung der Tafel I die im Artikel 72 entwickelte Regel befolgt haben.

316.

Nach diesen Prinzipien haben wir für alle Nenner von der Form p^μ unterhalb 1000 eine Tafel der notwendigen Perioden aufgestellt, die wir ganz oder auch in noch weiterer Fortsetzung bei gegebener Gelegenheit veröffentlichen werden. Hier möge die bis zu 100 nur fortgeführte Tafel III als Probe genügen, und wird eine Erklärung derselben kaum nötig sein. Für diejenigen Nenner, für welche 10 primitive Wurzel ist, stellt sie die Perioden der Brüche mit dem Zähler 1 dar (nämlich für 7, 17, 19, 23, 29, 47, 59, 61, 97), für die übrigen die f den Zählern 1, r, r^2, ..., r^{f-1} entsprechenden Perioden, welche durch die beigeschriebenen Zahlen (0), (1), (2), ... unterschieden sind; für die Basis r ist immer dieselbe primitive Wurzel genommen wie in Tafel I. Hiernach kann also die Periode eines jeden Bruches, dessen Nenner in dieser Tafel enthalten ist, mittelst der Vorschriften des vorigen Artikels abgeleitet werden, nachdem der Index des Zählers nach der Tafel I berechnet ist. Übrigens lässt sich für so kleine Nenner die Aufgabe ebenso leicht ohne die Tafel I erledigen, wenn man durch gewöhnliche Division soviel Anfangsziffern der gesuchten Mantisse berechnet, als nach Artikel 313 erforderlich sind, um sie von allen andern desselben Nenners unterscheiden zu können (für die Tafel III nicht mehr als 2), und sämtliche demselben Nenner entsprechende Perioden durchmustert, bis man zu jenen Anfangsziffern gelangt, welche den Anfang der Periode unzweifelhaft anzeigen; es muss jedoch darauf hingewiesen werden, dass jene Ziffern auch getrennt sein können, so dass die erste (oder mehrere) das Ende irgend einer Periode, die andere (oder die anderen) den Anfang derselben Periode bilden.

Beispiel. Man sucht die Periode des Bruches $\frac{12}{19}$. Hier hat man für den Modul 19 nach Tafel I ind. $12 = 2$ ind. $2 +$ ind. $3 = 39 \equiv 3$ (mod. 18) (Artikel 57). Somit muss man, da man für diesen Fall nur eine dem Zähler 1 entsprechende Periode hat, die drei ersten Ziffern derselben an das Ende setzen, woraus man die gesuchte Periode 631578947368421052 erhält. — Ebenso leicht hätte man den Anfang der Periode aus den beiden ersten Ziffern 63 gefunden.

Wenn man die Periode des Bruches $\frac{45}{53}$ haben will, so ist, für den Modul 53, ind. $45 = 2$ ind. $3 +$ ind. $5 = 49$; die Anzahl der Perioden ist hier

$4 = f$ und $49 = 12f + 1$; daher sind in der mit (1) bezeichneten Periode die 12 ersten Ziffern hinter die übrigen zu setzen, und die gesuchte Periode ist 8490566037735. Die Anfangsziffern 84 sind in diesem Falle in der Tafel von einander getrennt.

Wir bemerken noch, dass man mit Hülfe der Tafel III auch eine Zahl finden kann, welche für einen gegebenen Modul (der in ihr unter dem Namen Nenner enthalten ist) einem gegebenen Index entspricht, was zu zeigen wir schon im Artikel 59 versprochen haben. Denn offenbar kann man nach dem Vorhergehenden die Periode eines Bruches finden, dessen Zähler (auch wenn er unbekannt ist) der gegebene Index entspricht; es reicht jedoch hin, soviel Anfangsziffern dieser Periode aus der Tafel zu entnehmen, als der Nenner Ziffern hat; aus jenen leitet man dann nach Artikel 313 den Zähler oder die gesuchte dem gegebenen Index entsprechende Zahl her.

317.

Nach dem Vorhergehenden kann die Mantisse eines jeden Bruches, dessen Nenner eine Primzahl oder eine Potenz einer Primzahl innerhalb der Grenzen der Tafel ist, auf beliebig viele Ziffern ohne Rechnung abgeleitet werden; aber vermöge der Untersuchungen im Anfange dieses Abschnittes erstreckt sich die Anwendung der Tafel noch viel weiter und umfasst sämtliche Brüche, deren Nenner Producte aus Primzahlen oder Potenzen von Primzahlen innerhalb ihrer Grenzen sind. Denn da ein solcher Bruch in solche zerlegt werden kann, deren Nenner diese Factoren sind, und man diese in Decimalbrüche bis auf beliebig viele Stellen verwandeln kann, so bleibt nur übrig, die letzteren zu einer Summe zu vereinigen. Übrigens wird es kaum nötig sein, darauf hinzuweisen, dass die letzte Ziffer dieser Summe kleiner als die richtige werden kann; offenbar kann aber der Unterschied nicht auf soviele Einheiten ansteigen, als Teil-Brüche addiert werden, so dass es also gut sein wird, diese auf einige Stellen weiter zu berechnen, als der gegebene Bruch richtig werden soll. Beispielshalber betrachten wir den Bruch $\frac{6099380351}{1271808720} = F$*), dessen Nenner das Product aus den Zahlen 16, 9, 5, 49, 13, 47, 59 ist. Nach den oben angegebenen Principien findet man $F = 1 + \frac{11}{16} + \frac{4}{9} + \frac{4}{5} + \frac{22}{49} + \frac{5}{13} + \frac{7}{47} + \frac{52}{59}$, und diese Teilbrüche werden in folgender Weise in Decimalbrüche verwandelt:

*) Dieser Bruch ist einer von denen, welche der Quadratwurzel aus 23 möglichst nahe kommen, und zwar ist der Unterschied kleiner als 7 Einheiten in der zwanzigsten Decimalstelle.

$$
\begin{array}{rlll}
1 & = 1 & & \\
\frac{11}{16} & = 0{,}6875 & & \\
\frac{4}{5} & = 0{,}8 & & \\
\frac{4}{9} & = 0{,}4444444444 & 4444444444 & 44 \\
\frac{22}{49} & = 0{,}4489795918 & 3673469387 & 75 \\
\frac{5}{13} & = 0{,}3846153846 & 1538461538 & 46 \\
\frac{7}{47} & = 0{,}1489361702 & 1276595744 & 68 \\
\frac{52}{59} & = 0{,}8813559322 & 0338983050 & 84 \\
\hline
F & = 4{,}7958315233 & 1271954166 & 17
\end{array}
$$

Der Unterschied dieser Summe von dem richtigen Werte ist sicher kleiner als fünf Einheiten in der letzten zweiundzwanzigsten Decimalstelle, so dass dadurch die zwanzig ersten nicht geändert werden können. Führt man die Rechnung auf noch mehr Decimalstellen weiter, so ergeben sich für die beiden letzten Ziffern 17 die folgenden 1893936...

Übrigens wird jeder, auch ohne dass wir besonders darauf hinweisen, einsehen, dass diese Methode, gemeine Brüche in Decimalbrüche zu verwandeln, besonders für denjenigen Fall berechnet ist, wo man viele Decimalstellen haben will; denn wenn wenige genügen, kann die gewöhnliche Division oder die Rechnung mit Logarithmen meistens ebenso bequem angewendet werden.

318.

Da somit die Verwandlung solcher Brüche, deren Nenner aus mehreren verschiedenen Primzahlen zusammengesetzt sind, bereits auf denjenigen Fall zurückgeführt ist, wo der Nenner eine Primzahl oder eine Potenz einer Primzahl ist, so wollen wir nur noch Einiges über die Mantissen jener hinzufügen. Wenn der Nenner den Factor 2 oder 5 nicht enthält, so wird die Mantisse auch hier aus Perioden bestehen, da man auch für diesen Fall in der Reihe 10, 100, 1000,... schliesslich zu einem Gliede gelangt, welches der Einheit nach diesem Nenner congruent ist, und zugleich wird der Exponent dieses Gliedes, welcher nach Artikel 92 leicht bestimmt werden kann, die von dem Zähler nicht abhängende Grösse der Periode anzeigen, wofern der Zähler prim zum Nenner ist. — Ist aber der Nenner von der Form $2^\alpha 5^\beta N$, wo N eine zu 10 prime Zahl ist und α, β Zahlen bezeichnen, von denen wenigstens eine nicht gleich 0 ist, so wird die Mantisse des Bruches

erst nach den ersten α oder β Ziffern (je nachdem α oder β grösser ist) nur noch aus lauter Perioden bestehen, welche mit den Perioden der Brüche, deren Nenner N ist, hinsichtlich ihrer Länge übereinstimmen. Dies leitet man leicht daraus her, dass jener Bruch in zwei andere mit den Nennern $2^\alpha 5^\beta$ und N zerlegbar ist, von denen der erstere nach den ersten α oder β Ziffern abbricht. — Übrigens könnten wir über diesen Gegenstand noch viele andere Bemerkungen hinzufügen, besonders in Bezug auf die Kunstgriffe, welche man anwenden kann, um eine solche Tafel wie III möglichst schnell zu construieren; doch unterdrücken wir dies an dieser Stelle der Kürze wegen um so lieber, da mehreres hierher gehörige sowohl von Robertson a. a. O., als auch von Bernoulli (*Nouv. Mém. de l'Ac. de Berlin 1771, p. 273*) bereits angegeben worden ist.

Auflösung der Congruenz $x^2 \equiv A$ durch die Methode der Ausschliessung.

319.

Die Möglichkeit der Congruenz $x^2 \equiv A$ (mod. m), welche mit der unbestimmten Gleichung $x^2 = A + my$ übereinstimmt, haben wir im Abschnitt IV (Artikel 146) in einer Weise behandelt, dass nichts mehr zu wünschen übrig bleiben dürfte; hinsichtlich der Ermittlung der Unbekannten selbst aber haben wir schon oben (Artikel 152) bemerkt, dass indirecte Methoden den directen bei Weitem vorzuziehen seien. Ist m eine Primzahl (auf welchen Fall die übrigen leicht zurückgeführt werden können), so könnten wir zu diesem Zwecke die Tafel I der Indices (nach der Bemerkung im Artikel 316 in Verbindung mit Tafel III) benutzen, wie wir im Artikel 60 allgemeiner gezeigt haben; doch würde dieses Verfahren auf die Grenzen der Tafel beschränkt sein. Aus diesen Gründen wird hoffentlich die folgende allgemeine und bequeme Methode den Liebhabern der Arithmetik nicht unerwünscht sein.

Vor Allem bemerken wir, dass es genügt, wenn man nur diejenigen Werte von x hat, welche positiv und nicht grösser als $\frac{1}{2}m$ sind, da jeder andere irgend einem von diesen Werten selbst oder einem mit negativen Vorzeichen genommenen nach dem Modul m congruent ist; für einen solchen Wert von x aber wird der Wert von y notwendig zwischen den Grenzen $-\frac{A}{m}$ und $\frac{1}{4}m - \frac{A}{m}$ enthalten sein. Die Methode, welche sich unmittelbar darbietet, würde also darin bestehen, dass man für die einzelnen innerhalb dieser Grenzen liegenden Werte von y, deren Gesamtheit wir mit Ω bezeichnen, den Wert von $A + my$, den wir mit V bezeichnen, berechnet und nur diejenigen beibehält, für welche V ein Quadrat wird. Ist m eine kleine Zahl (z. B. unterhalb 40 gelegen), so ist dieser Versuch so kurz, dass er

einer Zusammenziehung kaum bedarf; wenn aber m gross ist, so kann die Arbeit durch die folgende Methode der Ausschliessung, soweit man will, abgekürzt werden.

320.

Es sei E eine beliebige ganze Zahl, welche prim zu m und grösser als 2 ist; ferner seien alle ihre verschiedenen (d. h. nach E incongruenten) quadratischen Reste: $a, b, c, \ldots$; endlich die Wurzeln der Congruenzen

$$A + my \equiv a, \quad A + my \equiv b, \quad A + my \equiv c, \ldots \pmod{E}$$

gleich $\alpha, \beta, \gamma, \ldots$ respective, die wir sämtlich positiv und kleiner als E annehmen dürfen. Wenn man nun y einen Wert beilegt, der irgend einer von den Zahlen $\alpha, \beta, \gamma, \ldots$ nach dem Modul E congruent ist, so wird der daraus entstehende Wert von $V = A + my$ irgend einer der Zahlen $a, b, c, \ldots$ congruent und somit Nichtrest von E sein; mithin kann er kein Quadrat sein. Hieraus geht hervor, dass aus Ω sogleich alle Zahlen als untauglich ausgeschlossen werden können, welche unter den Formen $Et + \alpha$, $Et + \beta$, $Et + \gamma, \ldots$ enthalten sind, und es wird genügen, den Versuch mit den übrigen, deren Complex Ω' sei, anzustellen. Bei jener Operation kann man der Zahl E den Namen **Exkludent** geben.

Nimmt man aber als Exkludenten eine andere passende Zahl E', so findet man auf ganz dieselbe Weise soviel Zahlen $\alpha', \beta', \gamma', \ldots$, als man verschiedene quadratische Nichtreste hat, denen y nach dem Modul E' nicht congruent sein kann. Daher kann man wiederum aus Ω' alle unter den Formen $E't + \alpha'$, $E't + \beta'$, $E't + \gamma', \ldots$ enthaltenen Zahlen weglassen. Auf diese Weise kann man fortfahren, indem man immer andere und andere Exkludenten anwendet, bis die Anzahl der Zahlen in Ω soweit verringert ist, dass es nicht schwieriger erscheint, mit allen übrigbleibenden den Versuch wirklich anzustellen, als neue Ausschliessungen vorzunehmen.

Beispiel. Ist die Gleichung $x^2 = 22 + 97y$ gegeben, so sind die Grenzen der Werte von y gleich $-\frac{22}{97}$ und $24\frac{1}{4} - \frac{22}{97}$, so dass (da die Untauglichkeit von 0 unmittelbar klar ist) Ω die Zahlen $1, 2, 3, \ldots, 24$ umfasst. Für $E = 3$ erhält man den einzigen Nichtrest $a = 2$; hieraus wird $\alpha = 1$; daher sind aus Ω alle Zahlen von der Form $3t + 1$ auszuschliessen; die Anzahl der übrigbleibenden Ω' ist 16. Ebenso erhält man für $E = 4$: $a = 2$, $b = 3$, woraus $\alpha = 0$, $\beta = 1$ wird; demnach sind alle Zahlen von der Form $4t$ und $4t + 1$ wegzulassen, und es bleiben die folgenden acht: 2, 3, 6, 11, 14, 15, 18, 23. Ebenso findet man für $E = 5$, dass die Zahlen von den Formen $5t$ und $5t + 3$ auszuschliessen sind; es bleiben also die folgenden: 2, 6, 11, 14. Der Exkludent 6 würde die Zahlen von den Formen $6t + 1$ und $6t + 4$ beseitigen; diese aber (welche mit den Zahlen von der Form $3t + 1$ übereinstimmen) sind schon weggelassen. Der Exkludent 7 beseitigt die Zahlen

von den Formen $7t+2, 7t+3, 7t+5$ und lässt die folgenden übrig: 6, 11, 14. Substituiert man diese für y, so ergiebt sich $V = 604, 1089, 1380$, von denen nur der zweite Wert ein Quadrat ist. Aus diesem wird $x = \pm 33$.

321.

Da die mit dem Exkludenten E angestellte Operation von den Werten von V, welche den Werten von y in Ω entsprechen, alle diejenigen ausschliesst, welche quadratische Nichtreste von E sind, die Reste derselben Zahl aber unberührt lässt, so sieht man leicht, dass sich die Anwendung von E und $2E$ in nichts unterscheidet, wenn E ungerade ist, da in diesem Falle E und $2E$ dieselben Reste und Nichtreste haben. Hieraus geht hervor, dass, wenn man der Reihe nach die Zahlen 3, 5, 7, ... als Exkludenten anwendet, die ungerademal geraden Zahlen 6, 10, 14, ... als unnütz übergangen werden müssen. Ferner ist ersichtlich, dass die doppelte mit den Exkludenten E, E' angestellte Operation alle diejenigen Werte von V beseitigt, welche Nichtreste entweder jeder der beiden Zahlen E, E' oder nur einer von ihnen sind, während diejenigen, welche Reste von beiden sind, zurückbleiben. Da nun in dem Falle, wo E und E' keinen gemeinschaftlichen Teiler haben, jene weggeworfenen Zahlen sämtlich Nichtreste und diese übrig bleibenden Reste des Products EE' sind, so ist klar, dass die Anwendung des Exkludenten EE' in diesem Falle ganz dasselbe bewirkt, wie die Anwendung von E und E', und dass somit jene nach dieser überflüssig wird. Daher kann man auch alle diejenigen Exkludenten übergehen, welche in zwei zu einander prime Factoren zerlegt werden können, und es reicht aus, diejenigen zu benützen, welche entweder (in m nicht aufgehende) Primzahlen oder Potenzen von Primzahlen sind. Endlich ist klar, dass nach der Anwendung des Exkludenten p^μ, welcher eine Potenz einer Primzahl p ist, der Exkludent p oder p^ν, falls $\nu < \mu$ ist, überflüssig wird; denn da p^μ unter den Werten von V nur Reste von sich übrig lässt, so werden um so weniger Nichtreste von p oder irgend einer niedrigeren Potenz p^ν noch vorhanden sein. Ist aber p oder p^ν schon vor p^μ angewendet worden, so kann dieses offenbar nur solche Werte von V beseitigen, welche gleichzeitig Reste von p (oder p^ν) und Nichtreste von p^μ sind; daher wird es ausreichen, nur solche Nichtreste von p^μ für $a, b, c, \ldots$ zu nehmen.

322.

Die Berechnung der Zahlen $\alpha, \beta, \gamma, \ldots$, welche irgend einem gegebenen Exkludenten E entsprechen, wird durch die folgenden Bemerkungen erheblich zusammengezogen. Es seien $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$ die Wurzeln der Congruenzen $my \equiv a$, $my \equiv b$, $my \equiv c, \ldots$ (mod. E) und k die Wurzel der Congruenz $my \equiv -A$, so wird offenbar $\alpha \equiv \mathfrak{A} + k$, $\beta \equiv \mathfrak{B} + k$, $\gamma \equiv \mathfrak{C} + k, \ldots$. Wenn wir nun $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$ wirklich durch Auflösung jener Congruenzen ermitteln müssten, so würde dieser Weg, die Zahlen $\alpha, \beta, \gamma, \ldots$ zu finden,

jedenfalls um nichts kürzer sein, als der, welchen wir oben gezeigt haben; doch ist jenes keineswegs notwendig. Wenn nämlich zunächst E eine Primzahl und m quadratischer Rest von E ist, so geht aus Artikel 98 hervor, dass $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$, welches die Werte der Ausdrücke $\frac{a}{m}, \frac{b}{m}, \frac{c}{m}, \ldots$ (mod. E) sind, verschiedene Nichtreste von E werden und daher mit $\alpha, \beta, \gamma, \ldots$ vollständig übereinstimmen, abgesehen von ihrer Reihenfolge, auf die hier nichts ankommt; wenn dagegen unter derselben Voraussetzung m Nichtrest von E ist, so werden die Zahlen $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$ mit sämtlichen quadratischen Resten nach Weglassung der 0 übereinstimmen. — Ist E das Quadrat einer (ungeraden) Primzahl, etwa gleich p^2, und ist schon p als Exkludent benutzt, so reicht es nach dem vorigen Artikel aus, für $a, b, c, \ldots$ diejenigen Nichtreste von p^2 zu nehmen, welche Reste von p sind, d. h. die Zahlen $p, 2p, 3p, \ldots, p^2-p$ (nämlich alle Zahlen unterhalb p^2, ausser 0, welche durch p teilbar sind); hieraus aber ist leicht ersichtlich, dass für $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$ ganz dieselben Zahlen, nur in anderer Reihenfolge, hervorgehen müssen. Analog wird es, wenn nach der Anwendung der Exkludenten p und p^2 $E=p^3$ gesetzt wird, ausreichen, für $a, b, c, \ldots$ die Producte der einzelnen Nichtreste von p mit p^2 zu nehmen, wodurch für $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$ entweder dieselben Zahlen, oder die Producte von p^2 in die einzelnen Reste von p ausser 0 hervorgehen werden, je nachdem m Rest oder Nichtrest von p ist. Allgemein nimmt man für E eine beliebige Potenz einer Primzahl, etwa p^μ, nachdem alle niedrigeren Potenzen bereits angewendet worden sind, so wird man für $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$ die Producte von $p^{\mu-1}$ entweder in sämtliche Zahlen, die kleiner als p sind, (0 immer ausgeschlossen), falls μ gerade ist, oder in alle unterhalb p liegende Nichtreste von p, falls μ ungerade und mRp ist, oder in alle Reste, falls mNp ist, erhalten. — Ist $E=4$ und daher $a=2$, $b=3$, so erhalten wir für $\mathfrak{A}, \mathfrak{B}$ entweder 2 und 3 oder 2 und 1, je nachdem $m\equiv 1$ oder $\equiv 3$ (mod. 4) ist. Wenn nach Anwendung des Exkludenten 4 $E=8$ gesetzt wird, so haben wir $\alpha=5$, woraus $\mathfrak{A}$ gleich 5, 7, 1, 3 wird, je nachdem $m\equiv 1$, 3, 5, 7 (mod. 8) ist. Allgemein aber, wenn E eine beliebig höhere Potenz von 2 etwa 2^μ ist, so muss man, nachdem die niedrigeren Potenzen von 2 bereits angewendet sind, $a=2^{\mu-1}$, $b=3\cdot 2^{\mu-2}$ setzen, wenn μ gerade ist, woraus $\mathfrak{A}=2^{\mu-1}$, $\mathfrak{B}=3\cdot 2^{\mu-2}$ oder $=2^{\mu-2}$ wird, je nachdem $m\equiv 1$ oder $\equiv 3$ ist; ist aber μ ungerade, so muss man $a=5\cdot 2^{\mu-3}$ setzen, wonach $\mathfrak{A}$ gleich dem Producte der Zahl $2^{\mu-3}$ in eine der Zahlen 5, 7, 1 oder 3 wird, je nachdem $m\equiv 1$, 3, 5, oder 7 (mod. 8) ist.

Übrigens werden Kundige sich leicht einen Apparat ersinnen, durch welchen die untauglichen Werte von y aus Ω mechanisch entfernt werden können, nachdem für so viele Exkludenten, als nötig erscheinen, die Zahlen $\alpha, \beta, \gamma, \ldots$ berechnet sind; doch können wir hierüber wie über andere Kunstgriffe, um die Arbeit abzukürzen, an dieser Stelle nicht handeln.

Lösung der unbestimmten Gleichung $mx^2+ny^2=A$ nach der Ausschliessungsmethode.

323.

Wir haben im Abschnitt V gezeigt, wie man sämtliche Darstellungen einer gegebenen Zahl A durch die binäre Form mx^2+ny^2 oder die Lösungen der unbestimmten Gleichung $mx^2+ny^2=A$ nach einer allgemeinen Methode findet, die an Kürze nichts zu wünschen übrig lassen dürfte, wenn man bereits sämtliche Werte des Ausdrucks $\sqrt{-mn}$ nach dem Modul A selbst und nach dem durch seine quadratischen Factoren geteilten Modul hat; hier werden wir aber für denjenigen Fall, wo mn positiv ist, eine Auflösung darlegen, die viel bequemer ist als die directe, wenn man für diese jene Werte erst vorher berechnen muss. Wir werden aber annehmen, dass die Zahlen m, n und A positiv und prim zu einander sind, da die übrigen Fälle auf diesen leicht zurückgeführt werden können. Offenbar genügt es auch, nur positive Werte von x, y zu suchen, da die übrigen aus diesen durch blosse Aenderung der Vorzeichen erhalten werden.

Es ist klar, dass x so beschaffen sein muss, dass $\frac{A-mx^2}{n}$, für welchen Bruch wir kurz V schreiben werden, positiv, ganz und eine Quadratzahl werde. Die erste Bedingung erfordert, dass x nicht grösser sei als $\sqrt{\frac{A}{m}}$; die zweite findet bereits von selbst statt, wenn $n=1$, sonst erfordert sie, dass der Wert des Ausdrucks $\frac{A}{m}$ (mod. n) quadratischer Rest von n sei; und bezeichnet man sämtliche verschiedene Werte des Ausdrucks $\sqrt{\frac{A}{m}}$ (mod. n) mit $\pm r, \pm r', \ldots$, so müssen die Werte von x unter einer der Formen $nt+r$, $nt-r$, $nt+r', \ldots$ enthalten sein. Es würde daher das einfachste sein, alle unterhalb der Grenze $\sqrt{\frac{A}{m}}$ liegenden Zahlen dieser Formen, deren Complex wir mit Ω bezeichnen, für x zu substituieren und nur diejenigen beizubehalten, für welche V ein Quadrat wird. Wir werden im folgenden Artikel zeigen, wie man dieses heuristische Verfahren, soweit man will, zusammenziehen kann.

324.

Die Methode der Ausschliessungen, nach welchen wir dies bewirken werden, besteht ebenso wie in der vorigen Untersuchung darin, dass man mehrere Zahlen, die wir auch hier Exkludenten nennen, nach Belieben annimmt, sodann untersucht, für welche Werte von x der Wert von V quadratischer Nichtrest von diesen Exkludenten wird, und derartige x aus Ω wegwirft. Durch eine Schlussreihe, die derjenigen, welche wir im Art. 321

auseinandergesetzt haben, vollkommen analog ist, geht hervor, dass nur solche Exkludenten anzuwenden sind, welche Primzahlen oder Potenzen von Primzahlen sind, und für einen Exkludenten der letzteren Art nur diejenigen Nichtreste desselben aus den Werten von V wegzulassen sind, welche Reste sämtlicher niederen Potenzen derselben Primzahl sind, wofern die Ausschliessung mit diesen bereits durchgeführt ist.

Es sei daher der Exkludent $E = p^\mu$ (einschliesslich desjenigen Falles, wo $\mu = 1$ ist), wo p eine in m nicht aufgehende Primzahl ist, und es werde angenommen*), dass p^ν die höchste Potenz derselben Primzahl sei, durch welche n teilbar ist. Es seien ferner $a, b, c, \ldots$ quadratische Nichtreste von E (und zwar sämtliche, wenn $\mu = 1$, die notwendigen oder diejenigen, welche Reste der niedrigeren Potenzen sind, wenn $\mu > 1$ ist). Berechnet man die Wurzeln der Congruenzen $mz \equiv A - na$, $mz \equiv A - nb$, $mz \equiv A - nc$, ... (mod. $Ep^\nu = p^{\mu+\nu}$), welche $\alpha, \beta, \gamma, \ldots$ sein mögen, so ergiebt sich leicht, dass, wenn für irgend einen Wert von x $x^2 \equiv \alpha$ (mod. Ep^ν) wird, der entsprechende Wert von $V \equiv a$ (mod. E) oder Nichtrest von E wird, und ebenso in Bezug auf die übrigen Zahlen $\beta, \gamma, \ldots$ Ebenso leicht ist umgekehrt ersichtlich, dass, wenn irgend ein Wert von x die Congruenz $V \equiv a$ (mod. E) zu Stande bringt, für ebendenselben $x^2 \equiv \alpha$ (mod. Ep^ν) ist, und dass somit sämtliche Werte von x, für welche x^2 keiner der Zahlen $\alpha, \beta, \gamma, \ldots$ nach dem Modul Ep^ν congruent ist, solche Werte von V hervorbringen, welche keiner der Zahlen, $a, b, c, \ldots$ nach dem Modul E congruent sind. Man wähle nun aus den Zahlen $\alpha, \beta, \gamma, \ldots$ sämtliche quadratischen Reste von Ep^ν, welche $g, g', g'', \ldots$ sein mögen, aus, berechne die Werte der Ausdrücke $\sqrt{g}$, $\sqrt{g'}$, $\sqrt{g''}$, ... (mod. Ep^ν) und nehme an, dass sich hieraus die Werte $\pm h$, $\pm h'$, $\pm h''$, ... ergeben. Wenn dies in dieser Weise geschehen, so ist klar, dass sämtliche Zahlen von den Formen $Ep^\nu t \pm h$, $Ep^\nu t \pm h'$, $Ep^\nu t \pm h''$, ... sicher aus Ω weggelassen werden können, und dass keinem nach dieser Ausschliessung in Ω noch verbleibenden Werte von x ein Wert von V entsprechen kann, der unter den Formen $Eu + a$, $Eu + b$, $Eu + c$, ... enthalten ist. Übrigens werden offenbar solche Werte von V schon an und für sich aus keinem Werte von x hervorgehen können, wenn sich unter den Zahlen $\alpha, \beta, \gamma, \ldots$ keine quadratischen Reste von Ep^ν vorfinden, und daher kann in diesem Falle die Zahl E als Exkludent nicht angewendet werden. — Derartige Exkludenten kann man so viele, als man will, anwenden, und daher können auf diese Weise die Zahlen in Ω nach Belieben verringert werden.

Wir wollen nun zusehen, ob man nicht auch Primzahlen, welche in m aufgehen, oder Potenzen solcher Primzahlen als Exkludenten benutzen kann. Ist B der Wert des Ausdrucks $\frac{A}{n}$ (mod. m), so ergiebt sich, dass

*) Der Kürze wegen fassen wir die beiden Fälle, in denen n durch p teilbar und nicht teilbar ist, zusammen; im letzteren muss man $\nu = 0$ setzen.

V stets B nach dem Modul m congruent wird, welcher Wert auch für x genommen werden möge, und dass somit zur Möglichkeit der gegebenen Gleichung notwendig erforderlich ist, dass B quadratischer Rest von m ist. Bezeichnet daher p irgend einen ungeraden Primteiler von m, welcher nach Voraussetzung in n und A und somit auch in B nicht aufgeht, so ist V für jeden beliebigen Wert von x Rest von p und daher auch von jeder beliebigen Potenz von p; mithin können p und seine Potenzen nicht als Excludenten genommen werden. — Aus ganz analogem Grunde ist, wenn m durch 8 teilbar ist, zur Möglichkeit der gegebenen Gleichung notwendig erforderlich, dass $B \equiv 1 \pmod{8}$ sei, weshalb auch für jeden beliebigen Wert von x: $V \equiv 1 \pmod{8}$ wird und somit die Potenzen von 2 als Excludenten nicht geeignet sind. — Wenn aber m durch 4 jedoch nicht durch 8 teilbar ist, so muss aus ähnlichem Grunde $B \equiv 1 \pmod{4}$ und der Wert des Ausdrucks $\frac{A}{n} \pmod{8}$ entweder 1 oder 5 sein; derselbe möge mit C bezeichnet werden. Man sieht ohne Schwierigkeit, dass für einen geraden Wert von x hier $V \equiv C$, für einen ungeraden $V \equiv C + 4 \pmod{8}$ wird, woraus hervorgeht, dass die geraden Werte zu verwerfen sind, wenn $C = 5$, die ungeraden, wenn $C = 1$ ist. — Ist endlich m durch 2 aber nicht durch 4 teilbar, so sei wie vorher C der Wert des Ausdrucks $\frac{A}{n} \pmod{8}$, welcher gleich 1, 3, 5 oder 7 ist, und D der Wert von $\frac{\frac{1}{2}m}{n} \pmod{4}$, welcher gleich 1 oder 3 ist. Da nun der Wert von V offenbar immer $\equiv C - 2Dx^2 \pmod{8}$ und daher für ein gerades x: $\equiv C$, für ein ungerades $\equiv C - 2D$ ist, so folgert man hieraus leicht, dass alle ungeraden Werte von x zu verwerfen sind, wenn $C = 1$, alle geraden, wenn $C = 3$ und $D = 1$ oder $C = 7$ und $D = 3$ ist, und dass für alle übrigbleibenden Werte $V \equiv 1 \pmod{8}$ oder also Rest einer jeden Potenz von 2 ist; in den übrigen Fällen aber, nämlich wenn $C = 5$ oder $C = 3$ und $D = 3$ oder $C = 7$ und $D = 1$ ist, wird $V \equiv 3$, 5 oder $7 \pmod{8}$, mag x gerade oder ungerade genommen werden, woraus erhellt, dass in diesen Fällen die gegebene Gleichung überhaupt keine Lösung besitzt.

Da wir übrigens auf ganz ähnliche Weise, wie wir hier den Wert von x durch Ausschliessungen finden lehrten, auch, mit den notwendigen Änderungen, den Wert von y hätten ableiten können, so kann man die Methode der Ausschliessung auf die Lösung des vorgelegten Problems stets auf zweierlei Art anwenden (falls nicht $m = n = 1$ ist, wo beide Arten zusammenfallen), von denen in den meisten Fällen diejenige vorzuziehen ist, für welche Ω eine kleinere Anzahl von Gliedern enthält, was sich leicht von vornherein abschätzen lässt. — Schliesslich wird es kaum nötig sein zu bemerken, dass, wenn nach einigen Ausschliessungen sämtliche Zahlen aus Ω herausgefallen sind, dies als ein sicheres Zeichen für die Unmöglichkeit der gegebenen Gleichung zu betrachten ist.

325.

Beispiel. Es sei gegeben die Gleichung $3x^2 + 455y^2 = 10857362$, die wir auf doppelte Weise lösen wollen, zuerst dadurch, dass wir die Werte von x, sodann dadurch, dass wir die Werte von y suchen. — Die Grenze jener ist in diesem Falle $\sqrt{3619120\frac{2}{3}}$, welche zwischen 1902 und 1903 fällt; der Wert des Ausdrucks $\frac{A}{3}$ (mod. 455) ist 354, und die Werte des Ausdrucks $\sqrt{354}$ (mod. 455) sind ± 82, ± 152, ± 173, ± 212. Hiernach besteht Ω aus den folgenden 33 Zahlen: 82, 152, 173, 212, 243, 282, 303, 373, 537, 607, 628, 667, 698, 737, 758, 828, 992, 1062, 1083, 1122, 1153, 1192, 1213, 1283, 1447, 1517, 1538, 1577, 1608, 1647, 1668, 1738, 1902. Die Zahl 3 kann in diesem Falle nicht als Exkludent genommen werden, da sie in m aufgeht. Für den Exkludenten 4 hat man $a = 2$, $b = 3$, woraus $\alpha = 0$, $\beta = 3$; $g = 0$ und als Werte des Ausdrucks $\sqrt{g}$ (mod. 4) die folgenden: 0 und 2; hieraus folgt, dass alle Zahlen von den Formen $4t$ und $4t + 2$, d. h. alle geraden Zahlen aus Ω wegzulassen sind; die (sechzehn) übrigen mögen mit Ω' bezeichnet werden. Für $E = 5$, welche Zahl auch in n aufgeht, erhalten wir als Wurzeln der Congruenzen $mz \equiv A - 2n$ und $mz \equiv A - 3n$ (mod. 25) die Werte 9 und 24, welche beide Reste von 25 sind, und die Werte der Ausdrücke $\sqrt{9}$ und $\sqrt{24}$ (mod. 25) werden ± 3, ± 7; lässt man aus Ω' sämtliche Zahlen von den Formen $25t \pm 3$, $25t \pm 7$ weg, so bleiben die folgenden zehn (Ω''): 173, 373, 537, 667, 737, 1083, 1213, 1283, 1517, 1577. Für $E = 7$ hat man als Wurzeln der Congruenzen $mz \equiv A - 3n$, $mz \equiv A - 5n$, $mz \equiv A - 6n$ (mod. 49) die Werte 32, 39, 18, welche sämtlich Reste von 49 sind, und als Werte der Ausdrücke $\sqrt{32}$, $\sqrt{39}$, $\sqrt{18}$ (mod. 49) die folgenden: ± 9, ± 23, ± 19; lässt man aus Ω'' die Zahlen von den Formen $49t \pm 9$, $49t \pm 23$, $49t \pm 19$ weg, so bleiben die folgenden fünf (Ω'''): 537, 737, 1083, 1213, 1517. Für $E = 8$ erhält man $a = 5$, somit $\alpha = 5$, welches Nichtrest von 8 ist; daher lässt sich der Exkludent 8 nicht anwenden. Die Zahl 9 ist aus demselben Grunde zu übergehen wie 3. Für $E = 11$ werden die Zahlen a, b, ... respective 2, 6, 7, 8, 10, ferner $\nu = 0$, somit die Zahlen α, β, ... $= 8$, 10, 5, 0, 1, von denen nur drei Reste von 11 sind, nämlich 0, 1, 5; hieraus ergiebt sich, dass aus Ω''' die Zahlen von den Formen $11t$, $11t \pm 1$, $11t \pm 5$ wegzulassen sind, so dass nur noch 537, 1083, 1213 übrig bleiben. Stellt man mit diesen die Probe an, so ergeben sich für V die Werte 21961, 16129, 14161 respective, von denen nur der zweite und dritte Quadrate sind. Daher besitzt die gegebene Gleichung zwei Lösungen durch positive Werte von x, y, nämlich $x = 1083$, $y = 127$ und $x = 1213$, $y = 119$.

Zweitens. Wenn man die andere der beiden Unbekannten derselben Gleichung durch Ausschliessungen ermitteln will, so setze man diese Gleichung unter die Form $455x^2 + 3y^2 = 10857362$, indem man x mit y

vertauscht, um sämtliche Bezeichnungen der Artikel 323, 324 beibehalten zu können. Die Grenze der Werte von x fällt hier zwischen 154 und 155; der Wert von $\frac{A}{m}$ (mod. n) ist 1, die Werte von $\sqrt{1}$ (mod. 3) sind $+1$ und -1. Daher enthält Ω alle Zahlen von den Formen $3t+1$ und $3t-1$, d. h. alle durch 3 nicht teilbaren Zahlen bis zu 154 einschliesslich, deren Anzahl gleich 103 ist; wendet man aber die oben gegebenen Prinzipien an, so findet man, dass für die Exkludenten 3; 4; 9; 11; 17; 19; 23 auszuschliessen sind die Zahlen von den Formen: $9t \pm 4$; $4t$, $4t \pm 2$ oder alle geraden Zahlen; $27t \pm 1$, $27t \pm 10$; $11t$, $11t \pm 1$, $11t \pm 3$; $17t \pm 3$, $17t \pm 4$, $17t \pm 5$, $17t \pm 7$; $19t \pm 2$, $19t \pm 3$, $19t \pm 8$, $19t \pm 9$; $23t$, $23t \pm 1$, $23t \pm 5$, $23t \pm 7$, $23t \pm 9$, $23t \pm 10$. Werden diese weggelassen, so bleiben übrig: 119, 227, welche beide für V ein Quadrat und dieselben Lösungen ergeben, zu denen wir oben gelangt waren.

326.

Die vorstehend angegebene Methode ist schon an und für sich so bequem. dass sie kaum etwas zu wünschen übrig lässt; trotzdem kann sie noch durch mannigfache Kunstgriffe, von denen wir hier nur einige kurz berühren können, erheblich zusammengezogen werden. Wir beschränken unsere Untersuchung auf denjenigen Fall, wo der Exkludent eine ungerade in A nicht aufgehende Primzahl oder eine Potenz einer solchen Primzahl ist, zumal da die übrigen Fälle entweder auf diesen zurückgeführt oder nach einer analogen Methode behandelt werden können. Nimmt man zunächst an, dass der Exkludent $E = p$ eine in m, n nicht aufgehende Primzahl sei, und dass die Werte der Ausdrücke $\frac{A}{m}$, $-\frac{na}{m}$, $-\frac{nb}{m}$, $-\frac{nc}{m}$, ... (mod. p) respective k, $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, ... seien, so findet man die Zahlen $\alpha, \beta, \gamma, \ldots$ mit Hülfe der Congruenzen: $\alpha \equiv k + \mathfrak{A}$, $\beta \equiv k + \mathfrak{B}$, $\gamma \equiv k + \mathfrak{C}$, ... (mod. p). Die Zahlen $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, ... können aber durch einen Kunstgriff, der dem im Artikel 322 benutzten ganz ähnlich ist, ohne Auflösung der Congruenzen ermittelt werden, und werden entweder mit sämtlichen Nichtresten oder mit sämtlichen Resten von p (ausser 0) übereinstimmen, je nachdem der Wert des Ausdrucks $-\frac{m}{n}$ (mod. p) oder (was hier auf dasselbe hinauskommt) die Zahl $-mn$ Rest oder Nichtrest von p ist. So wird in dem Beispiel II des vorigen Artikels für $E = 17$: $k = 7$; $-mn = -1365 \equiv 12$ ist Nichtrest von 17; daher sind die Zahlen $\mathfrak{A}$, $\mathfrak{B}$, ... respective 1, 2, 4, 8, 9, 13, 15, 16 und daher die Zahlen $\alpha, \beta, \ldots$ respective 8, 9, 11, 15, 16, 3, 5, 6; von diesen sind 8, 9, 11, 15, 16 Reste; somit werden $\pm h$, h', ... hier: ± 5, 3, 7, 4. — Diejenigen, welche öfters Gelegenheit haben, derartige Probleme zu lösen, werden sich die Sache erheblich erleichtern, wenn sie für mehrere Primzahlen p die Werte von $h, h', \ldots$, welche den einzelnen Werten von $k (1, 2, 3, \ldots, p-1)$ entsprechen, unter jeder der beiden Annahmen (nämlich dass $-mn$ Rest

oder Nichtrest von p sei) berechnen. Übrigens bemerken wir noch, dass die Anzahl der Zahlen $h, -h, h', \ldots$ stets gleich $\frac{1}{2}(p-1)$, wenn jede der beiden Zahlen k und $-mn$ Rest oder jede Nichtrest von p ist; ferner gleich $\frac{1}{2}(p-3)$, wenn die erste Rest, die zweite Nichtrest, und gleich $\frac{1}{2}(p+1)$ ist, wenn die erste Nichtrest, die zweite Rest ist; doch müssen wir den Beweis dieses Satzes, um nicht zu weitläufig zu werden, unterdrücken.

Was aber zweitens diejenigen Fälle betrifft, wo E eine in n aufgehende Primzahl oder die Potenz einer (ungeraden) Primzahl ist, mag dieselbe in n aufgehen oder nicht, so können dieselben noch einfacher behandelt werden. Alle diese Fälle behandeln wir gleichzeitig und setzen, unter Beibehaltung sämtlicher Bezeichnungen des Artikels 324, $n = n'p^\nu$, so dass n' durch p nicht teilbar ist. Die Zahlen $a, b, c, \ldots$ sind Producte der Zahl $p^{\mu-1}$ entweder in alle unterhalb p gelegene Zahlen (ausser 0) oder in alle Nichtreste von p unterhalb p, je nachdem μ gerade oder ungerade ist; dieselben mögen unbestimmt durch $up^{\mu-1}$ dargestellt werden. Ist k der Wert des Ausdrucks $\frac{A}{m}$ (mod. $p^{\mu+\nu}$), so ist derselbe durch p nicht teilbar, weil dieselbe Eigenschaft bei A vorausgesetzt wird; ferner ist klar, dass alle Zahlen $\alpha, \beta, \gamma, \ldots$ der Zahl k nach dem Modul p congruent werden und daher p^μ in Ω keine Ausschliessung bewirkt, wenn kNp ist; ist aber kRp und daher auch $kRp^{\mu+\nu}$, so sei r der Wert des Ausdrucks $\sqrt{k}$ (mod. $p^{\mu+\nu}$), welcher durch p nicht teilbar ist, und e der Wert von $-\frac{n'}{2mr}$ (mod. p); dann ist $\alpha \equiv r^2 + 2erap^\nu$ (mod. $p^{\mu+\nu}$), woraus leicht folgt, dass α Rest von $p^{\mu+\nu}$ ist und die Werte von $\sqrt{\alpha}$ (mod. $p^{\mu+\nu}$) werden: $\pm(r + eap^\nu)$. Demnach werden sämtliche Werte $h, h' h'', \ldots$ dargestellt durch $r + uep^{\mu+\nu-1}$. Endlich schliesst man hieraus leicht, dass die Zahlen $h, h', h'', \ldots$ entstehen durch Addition der Zahl r und der Producte der Zahl $p^{\mu+\nu-1}$ entweder in alle Zahlen unterhalb p (ausser 0), falls μ gerade ist, oder in alle Nichtreste von p unterhalb dieser Grenze, falls μ ungerade und eRp oder, was hier auf dasselbe hinauskommt, falls $-2mrn'Rp$ ist, oder in alle Reste (ausser 0), falls μ ungerade und $-2mrn'Np$ ist.

Übrigens wird man auch, sobald für die einzelnen Exkludenten, welche man anwenden will, die Zahlen $h, h', \ldots$ ermittelt sind, die Ausschliessung selbst auch durch mechanische Operationen bewirken können, wie sie sich jeder in diesen Dingen Erfahrene leicht selbst wird ersinnen können, wenn es sich der Mühe lohnen sollte.

Endlich müssen wir bemerken, dass jede Gleichung $ax^2 + 2bxy + cy^2 = M$, in welcher $b^2 - ac$ eine negative Zahl $= -D$ ist, leicht auf die im Vorstehenden betrachtete Form zurückgeführt werden kann. Bezeichnet man nämlich den grössten gemeinschaftlichen Teiler der Zahlen a, b mit m und setzt man:

$$a = ma', \; b = mb'; \; \frac{D}{m} = a'c - mb'^2 = n, \; a'x + b'y = x',$$

so ist jene Gleichung offenbar der folgenden Gleichung $mx'^2 + ny^2 = a'M$, welche nach den oben angegebenen Regeln gelöst werden kann, äquivalent. Von den Lösungen dieser sind aber nur die beizubehalten, in denen $x'-b'y$ durch a' teilbar ist, oder aus denen sich ganze Werte für x ergeben.

Andere Methode, die Congruenz $x^2 \equiv A$ zu lösen für den Fall, in welchem A negativ ist.

327.

Während die im Abschnitt V enthaltene directe Lösung der Gleichung $ax^2 + 2bxy + cy^2 = M$ die Werte des Ausdrucks $\sqrt{b^2 - ac}$ (mod. M) als bekannt voraussetzt, liefert umgekehrt in dem Falle, wo $b^2 - ac$ negativ ist, die im Vorhergehenden auseinandergesetze indirecte Auflösung eine sehr einfache Methode, jene Werte zu ermitteln, welche besonders für einen sehr grossen Wert von M der Methode des Artikels 322 u. ff. bei weitem vorzuziehen ist. Wir nehmen aber an, dass M eine Primzahl sei, oder dass wenigstens, wenn sie eine zusammengesetzte Zahl ist, ihre Factoren noch unbekannt seien; denn wenn man wüsste, dass die Primzahl p in M aufgeht, und $M = p^\mu M'$ ist, so dass M' den Factor p nicht mehr enthält, so würde es weit bequemer sein, die Werte des Ausdrucks $\sqrt{b^2 - ac}$ für die Moduln p^μ und M' einzeln (die ersteren aus den Werten für den Modul p, Artikel 101) zu ermitteln und aus der Combination dieser die Werte nach dem Modul M abzuleiten (Artikel 105).

Es sind daher sämtliche Werte des Ausdrucks $\sqrt{-D}$ (mod. M) zu suchen, wo D und M als positiv und M unter der Form der Teiler von $x^2 + D$ enthalten vorausgesetzt werden (Artikel 147 u. ff.), letzteres deshalb, weil sonst von vornherein feststände, dass keine Zahlen dem gegebenen Ausdruck genügen können. Es seien die gesuchten Werte, von denen stets je zwei einander entgegengesetzt sind, $\pm r, \pm r', \pm r'', \ldots$ und $D + r^2 = Mh$ $D + r'^2 = Mh'$, $D + r''^2 = Mh'', \ldots$; ferner mögen die Klassen, zu denen die Formen (M, r, h), $(M, -r, h)$, (M, r', h'), $(M, -r', h')$, (M, r'', h''), $(M, -r'', h''), \ldots$ gehören, respective mit $\mathfrak{C}, -\mathfrak{C}, \mathfrak{C}', -\mathfrak{C}', \mathfrak{C}'', -\mathfrak{C}'', \ldots$ und ihr Complex mit $\mathfrak{G}$ bezeichnet werden. Diese Klassen sind zwar, allgemein zu reden, als unbekannt zu betrachten; trotzdem ist ersichtlich, erstens dass sie sämtlich positiv und eigentlich primitiv sind, zweitens, dass sie sämtlich zu demselben Geschlechte gehören, dessen Character aus der Beschaffenheit der Zahl M, d. h. aus ihren Beziehungen zu den einzelnen Primteilern von D (und überdies zu 4 und 8, wenn diese nötig sind) leicht erkannt werden kann (Artikel 230). Da vorausgesetzt ist, dass M unter der Form der Teiler von $x^2 + D$ enthalten sei, so können wir von vornherein sicher sein, dass diesem Character notwendig ein positives, eigentlich primitives Geschlecht von Formen mit der Determinante $-D$ entspricht, ob-

gleich man vielleicht dem Ausdruck $\sqrt{-D}$ (mod. M) nicht genügen kann; da nun also dieses Geschlecht bekannt ist, kann man alle in ihm enthaltenen Klassen ermitteln; dieselben seien $C, C', C'', \ldots$ und ihr Complex G. Nun ist klar, dass jede einzelne Klasse $\mathfrak{C}, -\mathfrak{C}, \ldots$ mit irgend einer Klasse in G identisch sein muss; es kann auch geschehen, dass mehrere Klassen in $\mathfrak{G}$ unter sich und daher mit derselben Klasse in G identisch sind, und wenn G nur eine einzige Klasse enthält, so werden alle Klassen in $\mathfrak{G}$ mit dieser übereinstimmen. Wenn daher aus den Klassen $C, C', C'', \ldots$ die (einfachsten) Formen $f, f', f'', \ldots$ ausgewählt werden (je eine aus jeder), so wird sich von den einzelnen Klassen in $\mathfrak{G}$ je eine unter diesen vorfinden. Wenn nun $ax^2 + 2bxy + cy^2$ die in der Klasse $\mathfrak{C}$ enthaltene Form ist, so giebt es zwei zum Werte r gehörige Darstellungen der Zahl M durch sie, und zwar ist, wenn die eine $x = m$, $y = n$ ist, die andere $x = -m$, $y = -n$, nur der eine Fall, wo $D = 1$ ist, muss ausgenommen werden, da es in diesem vier Darstellungen giebt (Vgl. Artikel 180).

Hieraus schliesst man, dass, wenn man alle Darstellungen der Zahl M durch die einzelnen Formen $f, f', f'', \ldots$ (nach der im Vorstehenden angegebenen indirecten Methode) ermittelt und daraus die Werte des Ausdrucks $\sqrt{-D}$ (mod. M), zu welchen die einzelnen gehören, ableitet (Artikel 154), sämtliche Werte dieses Ausdrucks daraus erhalten werden und zwar jeder einzelne zweimal oder, falls $D = 1$ ist, viermal, womit die Aufgabe gelöst ist. Finden sich unter $f, f', f'', \ldots$ irgend welche Formen, durch welche M nicht dargestellt werden kann, so ist dies ein Zeichen, dass sie zu keiner Klasse in $\mathfrak{G}$ gehören und somit weggelassen werden müssen; wenn aber M durch keine von jenen Formen dargestellt werden kann, so muss notwendig $-D$ quadratischer Nichtrest von M sein.

Hinsichtlich dieser Operationen beachte man noch folgende Bemerkungen.

I. Es werden unter den Darstellungen der Zahl M durch die Formen $f, f', \ldots$, die wir hier anwenden, solche verstanden, in denen die Werte der Unbestimmten prim zu einander sind; erhält man irgend welche andern, in denen diese Werte einen gemeinschaftlichen Teiler haben (was nur dann der Fall sein kann, wenn μ^2 in M aufgeht, und sicher eintritt, wenn $-DR\frac{M}{\mu^2}$ ist), so müssen dieselben für den vorliegenden Zweck ganz weggelassen werden, obwohl sie in anderer Hinsicht nützlich sein können.

II. Unter sonst gleichen Umständen ist offenbar die Arbeit um so leichter, je kleiner die Anzahl der Klassen $f, f', f'', \ldots$ ist, und somit am kürzesten, wenn D eine von den 65 im Artikel 303 angegebenen Zahlen ist, für die es in den einzelnen Geschlechtern nur eine einzige Klasse giebt.

III. Da je zwei solche Darstellungen wie $x = m, y = n; x = -m, y = -n$ stets zu demselben Werte gehören, so reicht es offenbar aus, nur diejenigen Darstellungen zu betrachten, in denen y positiv ist. Derartige verschiedene

Darstellungen entsprechen daher immer verschiedenen Werten des Ausdruckes $\sqrt{-D}$ (mod. M), sodass die Anzahl aller verschiedenen Werte der Anzahl aller sich ergebenden Darstellungen dieser Art gleich ist (immer den Fall $D=1$ ausgenommen, in welchem jene die Hälfte dieser ist).

IV. Da man, sobald der eine der beiden entgegengesetzten Werte $+r$, $-r$ bekannt ist, auch sofort den andern kennt, so lassen sich die Operationen noch etwas abkürzen. Wird der Wert r aus der Darstellung der Zahl M durch eine in der Klasse C enthaltene Form gefunden, d. h. ist $\mathfrak{C}=C$, so wird sich offenbar der entgegengesetzte Wert $-r$ aus der Darstellung durch eine Form ergeben, welche in der zu C entgegengesetzten Klasse enthalten ist, die von der Klasse C verschieden ist, falls nicht etwa letztere ambig ist. Hieraus folgt, dass man, wenn nicht alle Klassen in G ambig sind, von den übrigen nur die Hälfte zu betrachten braucht, nämlich von je zwei entgegengesetzten nur die eine, während die andere wegzulassen ist, da aus ihr, wie man auch ohne Rechnung voraussetzen kann, sich Werte ergeben, welche denen, die die erstere liefert, entgegengesetzt sind. Ist aber C ambig, so werden sich aus ihr die beiden Werte r und $-r$ gleichzeitig ergeben; es wird nämlich, wenn aus C die ambige Form $ax^2+2bxy+cy^2$ ausgewählt wurde und der Wert r aus der Darstellung $x=m$, $y=n$ sich ergeben hat, der Wert $-r$ sich aus der folgenden $x=-m-\frac{2bn}{a}$, $y=n$ ergeben.

V. Für denjenigen Fall, in welchem $D=1$ ist, giebt es überhaupt nur eine Klasse, aus der, wie wir annehmen dürfen, die Form x^2+y^2 ausgewählt worden sei. Wenn nun der Wert r aus der Darstellung $x=m$, $y=n$ entsteht, so wird derselbe auch aus den Darstellungen $x=-m$, $y=-n$; $x=-m$, $y=n$; $x=m$, $y=-n$ und der entgegengesetzte $-r$ aus den Darstellungen $x=m$, $y=-n$; $x=-m$, $y=n$; $x=n$, $y=m$; $x=-n$, $y=-m$ sich ergeben. Daher genügt von diesen acht Darstellungen, welche nur eine Zerlegung geben, eine, wenn man nur dem daraus entstehenden Werte den entgegengesetzten associiert.

VI. Der Wert des Ausdrucks $\sqrt{-D}$ (mod. M), zu welchem die Darstellung $M=am^2+2bmn+cn^2$ gehört, ist nach Artikel 155: $\mu(mb+nc)-\nu(ma+nb)$ oder irgend eine diesem Werte nach dem Modul M congruente Zahl, wenn μ, ν so angenommen sind, dass $\mu m+\nu n=1$ ist. Bezeichnet man daher einen solchen Wert mit v, so ist:

$$mv \equiv \mu m(mb+nc)-\nu(M-mnb-n^2c) \equiv (\mu m+\nu n)(mb+nc)$$
$$\equiv mb+nc \pmod{M}.$$

Hieraus geht hervor, dass v der Wert des Ausdrucks $\frac{mb+nc}{m}$ (mod. M) ist, und auf ähnliche Weise findet man, dass v der Wert des Ausdrucks

$-\frac{ma+nb}{n}$ (mod. M) ist. Diese Formeln sind sehr häufig derjenigen, aus welcher sie abgeleitet sind, vorzuziehen.

328.

Beispiele. I. Man sucht sämtliche Werte des Ausdrucks $\sqrt{-1365}$ (mod. $5428681 = M$). Die Zahl M ist hier $\equiv 1, 1, 1, 6, 11$ (mod. 4, 3, 5, 7, 13) und daher unter der Form der Teiler von x^2+1, x^2+3, x^2-5 und unter der Form der Nichtteiler von x^2+7, x^2-13, also unter der Form der Teiler von x^2+1365 enthalten; der Character des Geschlechts, in welchem sich die Klassen $\mathfrak{G}$ vorfinden, ist 1, 4; $R3$; $R5$; $N7$; $N13$. In diesem Geschlecht ist nur eine einzige Klasse enthalten, aus welcher wir die Form $6x^2+6xy+229y^2$ auswählen. Um alle Darstellungen der Zahl M durch diese zu erhalten, setzen wir $2x+y=x'$, wodurch sie übergehen muss in $3x'^2+455y^2=2M$. Diese Gleichung besitzt vier Lösungen, in denen y positiv ist, nämlich $y=127$, $x'=\pm 1083$; $y=119$, $x'=\pm 1213$. Hieraus ergeben sich vier Lösungen der Gleichung $6x^2+6xy+229y^2=M$, in denen y positiv ist, nämlich:

x	478	-605	547	-666
y	127	127	119	119.

Die erste Lösung giebt für v den Wert des Ausdrucks $\frac{30517}{478}$ oder $-\frac{3249}{127}$ (mod. M), woraus man 2350978 findet; die zweite bringt den entgegengesetzten Wert -2350978, die dritte den Wert 2600262, die vierte den entgegengesetzten Wert -2600262 hervor.

II. Wenn die Werte des Ausdrucks $\sqrt{-286}$ (mod. $4272943 = M$) gesucht werden sollen, so findet man als Character des Geschlechts, in welchem die Klassen $\mathfrak{G}$ enthalten sind: 1 u. 7, 8; $R11$; $R13$; daher ist es das Hauptgeschlecht, in welchem drei Klassen enthalten sind, die durch die Formen (1, 0, 286), (14, 6, 23), (14, -6, 23) dargestellt werden; von diesen kann man die dritte, da sie der zweiten entgegengesetzt ist, weglassen. Durch die Form x^2+286y^2 findet man zwei Darstellungen der Zahl M, in denen y positiv ist, nämlich $y=103$, $x=\pm 1113$, aus denen sich die folgenden Werte des gegebenen Ausdrucks ergeben: 1493445, -1493445. Durch die Form (14, 6, 23) aber ist die Zahl M nicht darstellbar, woraus folgt, dass es ausser den beiden gefundenen Werten keine andern weiter giebt.

III. Ist der Ausdruck $\sqrt{-70}$ (mod. 997331) gegeben, so müssen die Klassen $\mathfrak{G}$ in einem Geschlechte enthalten sein, dessen Character 3 u. 5, 8; $R5$; $N7$ ist; in diesem findet sich nur eine einzige Klasse, deren repräsentierende Form (5, 0, 14) ist. Stellt man aber die Rechnung an, so findet man, dass die Zahl 997331 durch die Form (5, 0, 14) nicht darstellbar ist, weshalb -70 notwendig quadratischer Nichtrest jener Zahl ist.

Zwei Methoden, zusammengesetzte Zahlen von primen zu unterscheiden und ihre Factoren zu ermitteln.

329.

Dass die Aufgabe, die Primzahlen von den zusammengesetzten zu unterscheiden und letztere in ihre Primfactoren zu zerlegen, zu den wichtigsten und nützlichsten der gesamten Arithmetik gehört und die Bemühungen und den Scharfsinn sowohl der alten wie auch der neueren Geometer in Anspruch genommen hat, ist so bekannt, dass es überflüssig wäre, hierüber viele Worte zu verlieren. Trotzdem muss man gestehen, dass alle bisher angegebenen Methoden entweder auf sehr specielle Fälle beschränkt oder so mühsam und weitläufig sind, dass sie schon für solche Zahlen, welche die Grenzen der von verdienstvollen Männern aufgestellten Tafeln nicht überschreiten, d. h. für welche künstliche Methoden überflüssig sind, die Geduld sogar eines geübten Rechners ermüden, auf grössere Zahlen aber meistenteils kaum angewendet werden können. Obwohl aber jene Tafeln, die sich in aller Händen befinden, und die, wie wir hoffen dürfen, bald eine weitere Fortsetzung erfahren werden, in den meisten gewöhnlich vorkommenden Fällen jedenfalls ausreichen, so bietet sich doch dem erfahrenen Rechner nicht selten die Gelegenheit dar, aus der Zerlegung grosser Zahlen in Factoren grosse Vorteile zu ziehen, welche den mässigen Aufwand an Zeit reichlich wieder ausgleichen; ausserdem aber dürfte es die Würde der Wissenschaft erheischen, alle Hülfsmittel zur Lösung jenes so eleganten und berühmten Problems fleissig zu vervollkommnen. Aus diesen Gründen zweifeln wir nicht, dass die beiden folgenden Methoden, deren Wirksamkeit und Kürze wir durch eine lange Erfahrung bestätigen können, den Liebhabern der Arithmetik nicht unerwünscht sein werden. Übrigens ist es in der Natur der Aufgabe begründet, dass jede beliebige Methode fortwährend um so weitläufiger wird, je grösser die Zahlen sind, auf die sie angewandt wird; für die folgenden Methoden aber wachsen die Schwierigkeiten sehr langsam, und die aus sieben, acht, ja noch mehr Ziffern bestehenden Zahlen sind besonders nach der zweiten Methode stets mit glücklichem Erfolge und mit aller Schnelligkeit, die man billiger Weise für so grosse Zahlen erwarten kann, welche nach allen bisher bekannten Methoden eine auch dem unermüdlichen Rechner unerträgliche Arbeit erforderten, behandelt worden.

Bevor man die folgenden Methoden anwendet, ist es immer vorteilhaft, die Division irgend einer gegebenen Zahl durch einige der kleinsten Primzahlen, z. B. durch 2, 3, 5, 7, ... bis zu 19 oder noch weiter hinaus, zu versuchen, nicht nur, damit es nicht reut, eine solche Zahl, falls sie Divisor ist, durch subtile und künstliche Methoden erhalten zu haben, die man viel leichter durch blosse Division hätte finden können*), sondern auch deshalb,

*) Um so mehr, weil sich, allgemein zu reden, unter sechs Zahlen kaum eine findet, die nicht durch eine der Zahlen 2, 3, 5, ..., 19 teilbar wäre.

weil dann, wenn keine Division Erfolg hatte, die Anwendung der zweiten Methode sich der aus jenen Divisionen entstandenen Reste mit grossem Nutzen bedient. Soll z. B. die Zahl 314159265 in ihre Factoren zerlegt werden, so gelingt die Division durch 3 zweimal und sodann auch die Division durch 5 und 7, so dass man erhält: $314159265 = 9 \cdot 5 \cdot 7 \cdot 997331$ und es genügt, die Zahl 997331, die durch 11, 13, 17, 19 nicht teilbar befunden wird, einer eingehenderen Untersuchung zu unterwerfen. Analog werden wir von der gegebenen Zahl 43439448 den Factor 8 absondern und die künstlicheren Methoden auf den Quotienten 5428681 anwenden.

330.

Die Grundlage der **ersten Methode** bildet der Satz, dass jede positive oder negative Zahl, welche von einer andern Zahl M quadratischer Rest ist, auch quadratischer Rest jedes Teilers von M ist. Es ist allgemein bekannt, dass, wenn M durch keine Primzahl unterhalb $\sqrt{M}$ teilbar ist, M sicher eine Primzahl ist; dass aber, wenn alle Primzahlen unterhalb dieser Grenze, welche in M aufgehen, $p, q, \ldots$ sind, die Zahl M entweder aus diesen allein (und deren Potenzen) zusammengesetzt ist, oder nur einen einzigen andern Primfactor, der grösser als $\sqrt{M}$ ist, enthalten kann, welchen man findet, indem man M durch $p, q, \ldots$ so oft es geht dividiert. Bezeichnet man daher durch Ω den Complex aller Primzahlen unterhalb $\sqrt{M}$ (mit Ausschluss derjenigen, mit denen die Division bereits vergeblich versucht worden ist), so genügt es offenbar, wenn man alle in Ω enthaltenen Primteiler von M hat. Wenn man man nun irgend woher weiss, dass irgend eine (nichtquadratische) Zahl r quadratischer Rest von M ist, so kann sicher keine Primzahl, von welcher r Nichtrest ist, ein Teiler von M sein; daher wird man aus Ω sämtliche derartige Primzahlen (welche meistenteils ungefähr die Hälfte aller ausmachen) weglassen dürfen. Wenn überdies von einer andern nichtquadratischen Zahl r' bekannt ist, dass sie Rest von M ist, so wird man von den nach der ersten Ausschliessung in Ω übrig gebliebenen Primzahlen wiederum diejenigen ausschliessen können, von denen r' Nichtrest ist, und die wiederum ungefähr die Hälfte jener ausmachen, wofern die Reste r und r' unabhängig von einander sind (d. h., wenn nicht der eine notwendig an und für sich Rest aller Zahlen ist, von denen der andere Rest ist, was der Fall sein würde, wenn rr' ein Quadrat wäre). Sind noch andere Reste von M bekannt, $r'', r''', \ldots$, welche alle von den übrigen unabhängig sind*), so können mit den einzelnen analoge Ausschliessungen

*) Wenn das Product aus beliebig vielen Zahlen $r, r', r'', \ldots$ ein Quadrat ist, so ist jede von ihnen, z. B. r, Rest jeder (in keiner von ihnen aufgehenden) Primzahl, welche Rest der übrigen $r', r'', \ldots$ ist. Um also beliebig viele Reste als unabhängig betrachten zu können, darf kein ~~Quadrat~~ aus je zweien oder je dreien u. s. w. ein Quadrat sein. Product

vorgenommen werden, wodurch die Anzahl der Zahlen in Ω sehr rasch abnimmt, so dass bald entweder alle gestrichen sind, in welchem Falle M sicher eine Primzahl ist, oder nur so wenige übrigbleiben (unter denen sich offenbar alle Primteiler von M, wenn M solche hat, vorfinden), dass die Division durch sie ohne Mühe versucht werden kann. Bei einer Zahl, die eine Million nicht übersteigt, werden meistens sechs oder sieben, bei einer aus acht oder neun Ziffern bestehenden Zahl neun oder zehn Ausschliessungen vollauf genug sein. Nur über zwei Punkte müssen wir noch handeln, erstens, wie man passende und genügend viele Reste von M finden, zweitens, wie man die Ausschliessung selbst am bequemsten vornehmen kann. Jedoch wollen wir die Reihenfolge dieser Fragen umkehren, zumal da die zweite zeigen wird, was für Reste vornehmlich für diesen Zweck bequem sind.

331.

Wir haben im vierten Abschnitt ausführlich gezeigt, wie man die Primzahlen, von denen eine gegebene Zahl r (die wir durch kein Quadrat teilbar annehmen können) Rest ist, von denjenigen, von welchen sie Nichtrest ist, oder also wie man die Teiler des Ausdrucks $x^2 - r$ von den Nichtteilern unterscheiden kann, dass nämlich alle ersteren unter gewissen Formeln wie $rz + a$, $rz + b, \ldots$ oder wie $4rz + a$, $4rz + b, \ldots$ und die letzteren unter andern analogen Formeln enthalten seien. Ist r eine ziemlich kleine Zahl, so können die Ausschliessungen mit Hülfe dieser Formeln sehr bequem ausgeführt werden; z. B. sind alle Zahlen von der Form $4z + 3$, wenn $r = -1$, alle Zahlen von den Formen $8z + 3$, $8z + 5$, falls $r = 2$ ist, u. s. w. auszuschliessen. Da es aber nicht immer in unserer Macht steht, derartige Reste einer gegebenen Zahl zu finden, noch auch die Anwendung der Formeln für einen grossen Wert von r bequem genug ist, so ist es ein ungeheurer Vorteil und erleichtert die Mühe der Ausschliessung in erstaunlicher Weise, wenn man für eine hinreichend grosse Anzahl von positiven und negativen durch ein Quadrat nicht teilbaren Zahlen (r) bereits eine Tafel construiert hat, in welcher die Primzahlen, deren Reste jene einzelnen r sind, von denjenigen, deren Nichtreste sie sind, unterschieden sind. Eine solche Tafel kann in derselben Weise eingerichtet werden, wie die am Schlusse dieses Werkes angefügte und schon oben beschriebene Probe; damit dieselbe aber für den gegenwärtigen Zweck hinreichend grossen Nutzen gewähre, müssen die am Rande stehenden Primzahlen (Moduln) viel weiter, nämlich mindestens bis zu 1000 oder 10000 fortgesetzt werden; überdies wird die Bequemlichkeit noch bedeutend vermehrt werden, wenn man am Kopfe der Tafel auch die zusammengesetzten und negativen Zahlen aufnimmt, obwohl dies, wie aus dem vierten Abschnitt hervorgeht, nicht absolut notwendig ist. Am bequemsten aber wird der Gebrauch einer solchen Tafel, wenn die einzelnen Vertikalkolonnen, aus denen sie besteht, ausgeschnitten und auf Streifen von Blech oder auf (den Neper'schen ähnliche) Holz-

stäbchen aufgeklebt werden, so dass diejenigen, welche in jedem Falle erforderlich sind, d. h. welche den Zahlen $r, r', r'', \ldots$, den Resten der gegebenen in Factoren zu zerlegenden Zahl, entsprechen, für sich untersucht werden können. Werden diese in der richtigen Weise neben die erste Kolonne der Tafel (welche die Moduln darstellt) gelegt, d. h. so, dass die Plätze der einzelnen derselben Primzahl der ersten Kolonne entsprechenden Stäbchen mit dieser Primzahl in gerader Richtung liegen oder in dieselbe Horizontallinie fallen, so werden offenbar diejenigen Primzahlen, welche nach den Ausschliessungen vermittelst der Reste $r, r', r'', \ldots$ in Ω noch übrig bleiben, durch den blossen Anblick unmittelbar erkannt werden können; es werden nämlich diese übereinstimmen mit denjenigen in der ersten Kolonne, welchen in allen anliegenden Stäbchen Striche entsprechen, und es sind alle, bei welchen in irgend einem Stäbchen ein leerer Raum sich befindet, wegzulassen. Durch ein Beispiel wird dies hinreichend deutlich werden. Wenn man irgend woher weiss, dass die Zahlen $-6, +13, -14, +17, +37, -53$ Reste von 997331 sind, so muss man die erste Kolonne (welche in diesem Falle bis zu 997 fortgesetzt werden muss, d. h. bis zu der grössten Primzahl unterhalb $\sqrt{997331}$) und die Streifen, an deren Kopfe die Zahlen $-6, +13, \ldots$ stehen, nebeneinander legen. Wir geben hier einen Teil des auf diese Weise hervorgehenden Schemas:

	−6	+13	−14	+17	+37	−53
3	—	—	—		—	—
5	—		—			
7	—		—		—	
11	—				—	
13		—	—	—		—
17		—		—		—
19			—	—		—
23		—	—			—
			u. s. w.			
113		—	—			—
127	—	—	—	—	—	—
131	—	—	—			
			u. s. w.			

Wie man nun hier aus dem blossen Anblick erkennt, dass von denjenigen Primzahlen, welche in diesem Teil des Schemas enthalten sind, nur die Zahl 127 nach den Ausschliessungen vermittelst der Reste -6, $+13, \ldots$ in Ω übrig bleibt, so zeigt das ganze bis zur Zahl 997 erstreckte Schema, dass durchaus keine andere Zahl weiter in Ω übrig bleibt; versucht man aber die Division, so findet man, dass 997331 in der That durch 127 teilbar ist. Auf diese Weise ist daher jene Zahl in die Primfactoren $127 \cdot 7853$ zerlegt.

Übrigens geht aus dieser Auseinandersetzung zur Genüge hervor, dass nicht allzugrosse oder wenigstens in nicht allzugrosse Primzahlen zerlegbare Reste besonders vorteilhaft sind, da die unmittelbare Anwendung der Hülfstafel sich nicht über die am Kopfe befindlichen Zahlen hinaus erstreckt und die mittelbare Anwendung nur solche umfasst, welche in Factoren zerlegt werden können, die in der Tafel enthalten sind.

332.

Um die Reste der gegebenen Zahl M zu finden, werden wir drei verschiedene Methoden angeben, deren Auseinandersetzung wir zwei Bemerkungen vorausschicken, vermittelst deren man aus weniger geeigneten Resten einfachere ableiten kann. Erstens, wenn die Zahl ak^2, welche durch das Quadrat k^2 (das wir prim zu M voraussetzen) teilbar ist, Rest von M ist, so wird auch a Rest sein; daher sind die durch grosse Quadrate teilbaren Reste ebenso vorteilhaft, wie kleine, und wir werden somit voraussetzen, dass alle durch die nachstehenden Methoden gelieferten Reste sogleich von ihren quadratischen Factoren befreit seien. Zweitens, wenn zwei oder mehrere Zahlen Reste sind, so wird auch das Product aus ihnen ein Rest sein. Verbindet man diese Bemerkung mit der vorigen, so kann man sehr häufig aus mehreren Resten, welche nicht alle einfach genug sind, einen andern sehr einfachen ableiten, wofern nur jene viele gemeinsame Factoren haben. Aus diesem Grunde leisten auch solche Reste sehr gute Dienste, welche aus vielen nicht allzugrossen Factoren zusammengesetzt sind, und man wird gut thun, sogleich alle in ihre Factoren zu zerlegen. Die Bedeutung dieser Bemerkungen wird man besser durch Beispiele und häufigen Gebrauch als durch theoretische Vorschriften erkennen.

I. Die einfachste und für diejenigen, welche sich durch häufige Übung bereits einige Gewandtheit erworben haben, bequemste Methode besteht darin, dass man M oder allgemeiner irgend ein Vielfaches von M in zwei Teile zerlegt $km = a + b$ (mögen beide positiv oder der eine positiv, der andere negativ sein), deren Product mit verändertem Vorzeichen Rest von M sein wird; denn es ist $-ab \equiv a^2 \equiv b^2$ (mod. M) und daher $-abRM$. Die Zahlen a, b sind so anzunehmen, dass ihr Product durch ein grosses Quadrat teilbar und der Quotient entweder klein oder wenigstens in nicht zu grosse Factoren zerlegbar wird, was immer ohne Schwierigkeit ausgeführt werden kann. Besonders zu empfehlen ist es, für a entweder ein Quadrat oder ein doppeltes oder dreifaches u. s. w. Quadrat zu nehmen, welches von der Zahl M um eine entweder kleine oder in bequeme Factoren zerlegbare Zahl abweicht. So findet man z. B. $997331 = 999^2 - 2 \cdot 5 \cdot 67 = 994^2 + 5 \cdot 11 \cdot 13^2 = 2 \cdot 706^2 + 3 \cdot 17 \cdot 3^2 = 3 \cdot 575^2 + 11 \cdot 31 \cdot 4^2 = 3 \cdot 577^2 - 7 \cdot 13 \cdot 4^2 = 3 \cdot 578^2 - 7 \cdot 19 \cdot 37 = 11 \cdot 299^2 + 2 \cdot 3 \cdot 5 \cdot 29 \cdot 4^2 = 11 \cdot 301^2 + 5 \cdot 12^2$, u. s. w. Hieraus erhält man die folgenden Reste: $2 \cdot 5 \cdot 67$, $-5 \cdot 11$, $-2 . 3 \cdot 17$, $-3 \cdot 11 \cdot 31$, $3 \cdot 7 \cdot 13$, $3 \cdot 7 \cdot 19 \cdot 37$, $-2 \cdot 3 \cdot 5 \cdot 11 \cdot 29$; die letzte Zerlegung liefert den Rest $-5 \cdot 11$, den wir schon haben. An Stelle der

Reste $-3 \cdot 11 \cdot 31$, $-2 \cdot 3 \cdot 5 \cdot 11 \cdot 29$ kann man die folgenden nehmen: $3 \cdot 5 \cdot 31$, $2 \cdot 3 \cdot 29$, welche aus ihrer Combination mit $-5 \cdot 11$ entstehen.

II. Die zweite und dritte Methode gründet sich darauf, dass, wenn zwei binäre Formen (A, B, C), (A', B', C') mit derselben Determinante M oder $-M$ oder allgemeiner $\pm kM$ zu demselben Geschlechte gehören, die Zahlen AA', AC', $A'C$ Reste von kM sind; dies erkennt man ohne Schwierigkeit daraus, dass jede characteristische Zahl der einen Form, etwa m, auch eine characteristische Zahl der andern ist und somit mA, mC, mA', mC' sämtlich Reste von kM sind. Ist daher (a, b, a') eine reducierte Form mit der positiven Determinante M oder allgemeiner kM und sind (a', b', a''), (a'', b'', a'''), ... Formen aus ihrer Periode und somit ihr äquivalent und um so mehr unter demselben Geschlecht mit ihr enthalten, so sind die Zahlen aa', aa'', aa''', ... sämtlich Reste von M. Die Berechnung einer grossen Anzahl von Formen einer solchen Periode kann man mit Hülfe des Algorithmus im Artikel 187 sehr leicht durchführen; die einfachsten Reste ergeben sich meistens, wenn man $a = 1$ setzt; diejenigen, welche zu grosse Factoren enthalten, sind zu verwerfen. Nachstehend sieht man die Anfänge der Perioden der Formen $(1, 998, -1327)$ und $(1, 1412, -918)$, deren Determinanten 997331 und 1994662 sind:

$(1, 998, -1327)$	$(1, 1412, -918)$
$(-1327, 329, 670)$	$(-918, 1342, 211)$
$(670, 341, -1315)$	$(211, 1401, -151)$
$(-1315, 974, 37)$	$(-151, 1317, 1723)$
$(37, 987, -626)$	$(1723, 406, -1062)$
$(-626, 891, 325)$	$(-1062, 656, 1473)$
$(325, 734, -1411)$	$(1473, 817, -901)$
$(-1411, 677, 382)$	$(-901, 985, 1137)$
$(382, 851, -715)$	u. s. w.
u. s. w.	

Es sind daher Reste der Zahl 997331 sämtliche Zahlen -1327, 670, ... Lässt man aber diejenigen fort, welche zu grosse Factoren enthalten, so hat man die folgenden: $2 \cdot 5 \cdot 67$, 37, 13, $-17 \cdot 83$, $-5 \cdot 11 \cdot 13$, $-2 \cdot 3 \cdot 17$, $-2 \cdot 59$, $-17 \cdot 53$. Den Rest $2 \cdot 5 \cdot 67$, sowie den Rest $-5 \cdot 11$, welcher aus der Combination des dritten mit dem fünften entsteht, hatten wir schon oben gefunden.

III. Ist C irgend eine von der Hauptklasse verschiedene Klasse der Formen mit der negativen Determinante $-M$ oder allgemeiner $-kM$, und ist $2C$, $3C$, ... ihre Periode (Artikel 307), so gehören die Klassen $2C$, $4C$, ... zum Hauptgeschlecht, die Klassen $3C$, $5C$, ... aber zu demselben Geschlecht wie C. Wenn daher (a, b, c) die (einfachste) Form aus C und (a', b', c') eine Form aus irgend einer Klasse jener Periode, etwa aus nC, ist, so wird entweder a' oder aa' Rest von M sein, je nachdem n gerade oder ungerade ist (im ersteren Falle offenbar auch c', im letzteren ac', ca'

und cc'). Die Entwicklung der Periode, d. h. der einfachsten Formen in ihrer Klasse, lässt sich mit erstaunlicher Leichtigkeit ausführen, wenn a sehr klein ist, zumal im Fall $a = 3$, den man immer herbeiführen kann, wenn man $kM \equiv 2 \pmod{3}$ macht. Nachstehend sieht man den Anfang der Periode der Klasse, in welcher die Form (3, 1, 332444) enthalten ist.

$C = (3, \quad 1, 332444)$	$6C = (729, -209, 1428)$
$2C = (9, -2, 110815)$	$7C = (476, \quad 209, 2187)$
$3C = (27, \quad 7, \quad 36940)$	$8C = (1027, \quad 342, 1085)$
$4C = (81, \quad 34, \quad 12327)$	$9C = (932, -437, 1275)$
$5C = (243, \quad 34, \quad 4109)$	$10C = (425, \quad 12, 2347)$.

Hieraus ergeben sich die Reste (mit Beiseitelassung der untauglichen): $3 \cdot 476$, 1027, 1085, 425 oder (wenn man die quadratischen Factoren weglässt): $3 \cdot 7 \cdot 17$, $13 \cdot 79$, $5 \cdot 7 \cdot 31$, 17, und verbindet man diese in angemessener Weise mit den acht in II gefundenen, so findet man leicht die folgenden zwölf: $-2 \cdot 3$, 13, $-2 \cdot 7$, 17, 37, -53, $-5 \cdot 11$, 79, -83, $-2 \cdot 59$, $-2 \cdot 5 \cdot 31$, $2 \cdot 5 \cdot 67$. Die sechs ersten sind dieselben, deren wir uns im Artikel 331 bedient haben. Es hätten noch die Reste 19 und -29 hinzugefügt werden können, wenn wir auch diejenigen hätten anwenden wollen, die in I gefunden sind; die übrigen dort erhaltenen Reste sind von den hier abgeleiteten bereits abhängig.

333.

Die **zweite Methode**, eine gegebene Zahl M in Factoren zu zerlegen, geht aus von der Betrachtung der Werte eines Ausdrucks wie $\sqrt{-D} \pmod{M}$ und stützt sich auf folgende Bemerkungen:

I. Ist M eine Primzahl oder eine Potenz einer (ungeraden in D nicht aufgehenden) Primzahl, so ist $-D$ Rest oder Nichtrest von M, je nachdem M in der Form der Teiler oder in der Form der Nichtteiler von $x^2 + D$ enthalten ist, und im ersteren Falle besitzt der Ausdruck $\sqrt{-D} \pmod{M}$ nur zwei verschiedene Werte, welche entgegengesetzt sind.

II. Ist aber M eine zusammengesetzte Zahl, etwa $= pp'p'' \ldots$, wo p, $p', p'', \ldots$ (ungerade in D nicht aufgehende verschiedene) Primzahlen oder Potenzen solcher Primzahlen bezeichnen, so ist $-D$ nur dann Rest von M, wenn es Rest der einzelnen $p, p', p'', \ldots$ ist, d. h. wenn diese Zahlen sämtlich in den Formen der Teiler von $x^2 + D$ enthalten sind. Bezeichnet man aber die Werte des Ausdrucks $\sqrt{-D}$ nach den Moduln $p, p', p'', \ldots$ bezüglich mit $\pm r, \pm r' \pm r'', \ldots$, so entstehen sämtliche Werte desselben Ausdrucks nach dem Modul M, wenn man die Zahlen sucht, welche nach p entweder $\equiv r$ oder $\equiv -r$, nach p' entweder $\equiv r'$ oder $\equiv -r'$, u. s. w. sind, so dass also ihre Anzahl gleich 2^μ wird, wenn μ die Anzahl der Zahlen $p, p', p'', \ldots$ bezeichnet. Wenn nun diese Werte $R, -R, R', -R', R'', \ldots$ sind, so ist von selbst $R \equiv R$ nach allen Zahlen $p, p', p'', \ldots$; aber nach keiner $R \equiv -R$,

so dass der grösste gemeinschaftliche Teiler der Zahlen M und $R-R$ gleich M und der grösste gemeinschaftliche Teiler von M und $R+R$ gleich 1 ist; zwei Werte aber, die weder identisch noch entgegengesetzt sind, wie z. B. R und R' werden notwendig nach einer oder mehreren von den Zahlen $p, p', p'', \ldots$ aber nicht nach allen congruent sein und nach den übrigen ist $R \equiv -R'$; daher ist das Product jener der grösste gemeinschaftliche Teiler der Zahlen M und $R-R'$, und das Product dieser der grösste gemeinschaftliche Teiler der Zahlen M und $R+R'$. Hieraus folgt leicht, dass, wenn alle grössten gemeinschaftlichen Teiler von M und der Differenzen zwischen den einzelnen Werten des Ausdrucks $\sqrt{-D}$ (mod. M) und irgend eines gegebenen Wertes berechnet werden, der Complex derselben die Zahlen $1, p, p', p'', \ldots$ sowie die Producte von je zweien, je dreien u. s. w. dieser Zahlen enthält. Auf diese Weise ist man daher im Stande, aus den Werten jenes Ausdrucks die Zahlen $p, p', p'', \ldots$ abzuleiten.

Da übrigens die Methode des Artikels 327 diese einzelnen Werte auf die Werte von Ausdrücken von der Form $\frac{m}{n}$ (mod. M) reduciert, so dass der Nenner n zu M prim ist, so ist es für den gegenwärtigen Zweck nicht einmal notwendig, diese selbst zu berechnen. Denn der grösste gemeinschaftliche Divisor der Zahl M und der Differenz zwischen R und R', welche mit $\frac{m}{n}, \frac{m'}{n'}$ übereinstimmen, ist offenbar auch grösster gemeinschaftlicher Teiler von M und $nn'(R-R')$ oder von M und $mn'-m'n$, da dieser Zahl die Zahl $nn'(R-R')$ nach dem Modul M congruent ist.

334.

Die vorstehenden Bemerkungen lassen sich auf das vorliegende Problem in doppelter Weise anwenden; die erstere entscheidet nicht nur, ob eine gegebene Zahl M eine Primzahl oder eine zusammengesetzte Zahl ist, sondern sie liefert auch in diesem Falle die Factoren selbst; die letztere aber verdient insofern den Vorzug, als sie meistens eine einfachere Rechnung gestattet, indessen giebt sie nicht immer, wofern sie nicht mehrmals wiederholt wird, die Factoren der zusammengesetzten Zahlen selbst, jedoch unterscheidet auch sie die zusammengesetzten Zahlen von den Primzahlen.

I. Man suche eine negative Zahl $-D$, welche quadratischer Rest von M ist, zu welchem Zwecke man die im Artikel 332 unter I und II angegebenen Methoden benutzen kann. An sich zwar ist es willkürlich, welchen Rest man wählt, auch ist es hier nicht wie in der vorigen Methode erforderlich, dass D eine kleine Zahl sei; indessen wird die Rechnung um so kürzer sein, je kleiner die Anzahl der in den einzelnen eigentlich primitiven Geschlechtern mit der Determinante $-D$ enthaltenen Klassen binärer Formen ist, so dass besonders solche Reste, welche unter den 65 Zahlen des Artikels 303 enthalten sind, wenn sich solche darbieten, günstig sind. So würde für $M = 997331$ von allen oben ermittelten negativen Resten

der Rest -102 am geeignetsten sein. Man entwickle sodann alle von einander verschiedenen Werte des Ausdrucks $\sqrt{-D}$ (mod. M); wenn sich nur zwei (entgegengesetzte) ergeben, so ist M sicher eine Primzahl oder eine Potenz einer Primzahl; wenn dagegen mehrere, etwa 2^μ, hervorgehen, so ist M zusammengesetzt aus μ verschiedenen Primzahlen oder Potenzen von Primzahlen, und diese Factoren können nach der Methode des vorigen Artikels gefunden werden. Ob aber diese Factoren Primzahlen oder Potenzen von Primzahlen sind, lässt sich nicht nur an sich sehr leicht entscheiden, es giebt auch das Verfahren selbst, nach welchem die Werte des Ausdrucks $\sqrt{-D}$ gefunden werden, sämtliche Primzahlen, von denen irgend eine Potenz in M aufgeht, unmittelbar an. Ist nämlich M durch das Quadrat einer Primzahl π teilbar, so wird jene Rechnung sicher auch eine oder mehrere Darstellungen der Zahl M, $M = am^2 + 2bmn + cn^2$, von der Art zum Vorschein bringen, dass in ihnen der grösste gemeinschaftliche Teiler der Zahlen m, n gleich π ist (und zwar deshalb, weil in diesem Falle $-D$ auch Rest von $\frac{M}{\pi^2}$ ist). Wenn sich aber keine Darstellung ergiebt, in welcher m und n einen gemeinschaftlichen Teiler haben, so ist dies ein sicheres Zeichen, dass M durch kein Quadrat teilbar ist und somit alle Zahlen p, p', p'', ... Primzahlen sind.

Beispiel. Nach der oben angegebenen Methode findet man vier Werte des Ausdrucks $\sqrt{-408}$ (mod. 997331), welche mit den Werten $\pm\frac{1664}{113}$, $\pm\frac{2824}{3}$ übereinstimmen; als grösste gemeinschaftliche Factoren der Zahl 997331 und der Zahlen $3 \cdot 1664 - 113 \cdot 2824$ und $3 \cdot 1664 + 113 \cdot 2824$ oder der Zahlen 314120 und 324104 findet man 7853 und 127, daher $997331 = 127 \cdot 7853$, wie oben.

II. Man nehme irgend eine negative Zahl $-D$ von der Art an, dass M in der Form der Teiler von $x^2 + D$ enthalten ist. An sich ist es willkürlich, was für eine Zahl dieser Art man nimmt; der Bequemlichkeit halber aber muss man besonders darauf sehen, dass die Anzahl der Klassen in den Geschlechtern mit der Determinante $-D$ möglichst klein ist. Übrigens ist die Ermittlung einer solchen Zahl keinen Schwierigkeiten unterworfen, wenn man sie durch Probieren versucht; denn meistenteils ist M unter einer beträchtlichen Anzahl probierter Zahlen ungefähr für ebenso viele in der Form der Teiler, wie in der Form der Nichtteiler enthalten. Daher ist es am zweckmässigsten, den Versuch mit den 65 Zahlen des Artikels 303 (und zwar mit den grössten) zu beginnen und erst, wenn es sich träfe, dass keine derselben geeignet ist (was jedoch allgemein zu reden unter 16384 Fällen nur einmal eintritt), zu andern fortzuschreiten, bei denen je zwei Klassen in den einzelnen Geschlechtern enthalten sind. — Sodann ermittle man die Werte des Ausdrucks $\sqrt{-D}$ (mod. M) und leite, wenn man solche

Werte findet, die Factoren von M in ganz derselben Weise daraus her wie oben. Wenn aber keine solchen Werte hervorgehen und daher $-D$ Nichtrest von M ist, so wird sicher M weder eine Primzahl noch eine Potenz einer Primzahl sein können. Will man nun in diesem Falle die Factoren selbst haben, so muss man entweder dieselbe Operation wiederholen, indem man andere Werte für D nimmt, oder zu einer andern Methode seine Zuflucht nehmen.

Stellt man z. B. den Versuch mit der Zahl 997331 an, so findet man, dass dieselbe in der Form der Nichtteiler von x^2+1848, x^2+1365, x^2+1320, dagegen in der Form der Teiler von x^2+840 enthalten ist; als Werte des Ausdruckes $\sqrt{-840}$ (mod. 997331) erhält man die Ausdrücke $\pm\frac{1272}{163}$, $\pm\frac{3288}{125}$, woraus man dieselben Factoren ableitet wie oben. — Wer mehr Beispiele wünscht, möge Artikel 328 zu Rate ziehen, wo das erste Beispiel zeigt, dass $5428681 = 307 \cdot 17683$, das zweite, dass 4272943 eine Primzahl, das dritte, dass 997331 sicher aus mehreren Primzahlen zusammengesetzt ist.

Übrigens gestatteten es die Grenzen dieses Werkes nur, die Hauptmomente beider Methoden, die Factoren zu ermitteln, darzulegen; eine ausführlichere Untersuchung nebst mehreren Hülfstafeln und andern Hülfsmitteln behalten wir uns für eine andere Gelegenheit vor.

Siebenter Abschnitt.

Über diejenigen Gleichungen, von denen die Teilung des Kreises abhängt.

335.

Unter den glänzendsten Erweiterungen, welche die Mathematik durch die Arbeiten neuerer Geometer erfahren hat, nimmt die Theorie der vom Kreise abhängenden Functionen ohne Zweifel einen besonders hervorragenden Platz ein. Auf diese wunderbare Art von Grössen, zu denen man bei den verschiedenartigsten Untersuchungen gelangt und deren Hülfe kein Teil der gesamten Mathematik entbehren kann, haben die grössten neueren Geometer ihren Fleiss und ihren Scharfsinn in so beharrlicher Weise verwandt und eine so ausgedehnte Disciplin daraus gebildet, dass man kaum hätte erwarten können, dass irgend ein Teil dieser Theorie, geschweige denn ein elementarer und gleichsam an der Schwelle liegender Teil, noch wichtigerer Erweiterungen fähig sei. Ich meine die Theorie der trigonometrischen Functionen, welche Bogen entsprechen, die mit dem Umfange commensurabel sind, oder die **Theorie der regulären Polygone**; der gegenwärtige Abschnitt wird zeigen, ein wie geringer Teil derselben bisher zu Tage gefördert wurde. Der Leser könnte sich wundern, dass eine solche Untersuchung gerade in diesem Werke, das einem beim ersten Anblick ganz heterogenen Gegenstande vorzugsweise gewidmet ist, angestellt wird; doch wird die Abhandlung selbst hinreichend klarlegen, in welchem innigen Zusammenhange dieser Gegenstand mit der höheren Arithmetik steht.

Übrigens erstrecken sich die Prinzipien der Theorie, an deren Auseinandersetzung wir jetzt gehen, viel weiter, als sie hier ausgedehnt werden. Denn nicht allein auf die Kreisfunctionen lassen sie sich anwenden, sondern noch auf viele andere transcendente Functionen, z. B. auf diejenigen, welche von dem Integral $\int \frac{dx}{\sqrt{1-x^4}}$ abhängen, und ausserdem auch auf verschiedene Arten von Congruenzen; da wir aber über jene transcendenten Functionen ein umfassendes besonderes Werk vorbereiten, über die Congruenzen aber

in der Fortsetzung der arithmetischen Untersuchungen ausführlich gehandelt werden wird, so schien es uns gut, an dieser Stelle nur die Kreisfunctionen zu betrachten. Ja auch diese, die wir mit der grössten Allgemeinheit behandeln könnten, werden wir durch die in den folgenden Artikeln darzulegenden Hülfsmittel auf den einfachsten Fall reducieren, einerseits der Kürze wegen, andererseits damit die vollständig neuen Prinzipien dieser Theorie um so leichter verstanden werden.

Die Untersuchung wird auf den einfachsten Fall zurückgeführt, in welchem die Anzahl der Teile, in welche der Kreis geteilt werden soll, eine Primzahl ist.

336.

Bezeichnet man die Peripherie des Kreises oder vier rechte Winkel mit P und nimmt man an, dass m, n ganze Zahlen seien und n das Product aus den zu einander primen Factoren a, b, c, ..., so lässt sich der Winkel $A = \frac{mP}{n}$ nach Artikel 310 auf die folgende Form bringen: $A = \left(\frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \cdots\right)P$, und die ihm entsprechenden trigonometrischen Functionen werden aus den zu den Teilen $\frac{\alpha P}{a}$, $\frac{\beta P}{b}$, $\cdots$ gehörigen Functionen nach bekannten Methoden hergeleitet. Da man nun für a, b, c, ... Primzahlen oder Potenzen von Primzahlen nehmen kann, so genügt es offenbar, die Teilung des Kreises in Teile, deren Anzahl eine Primzahl oder die Potenz einer Primzahl ist, zu betrachten, und das Polygon von n Seiten wird aus den Polygonen von a, b, c, ... Seiten sogleich erhalten werden. Indessen werden wir an dieser Stelle unsere Untersuchung auf denjenigen Fall beschränken, wo der Kreis in Teile geteilt werden soll, deren Anzahl eine (ungerade) Primzahl ist, und zwar werden wir hierbei besonders von folgendem Grunde geleitet. Bekanntlich werden die dem Winkel $\frac{mP}{p^2}$ entsprechenden Kreisfunctionen aus den zu $\frac{mP}{p}$ gehörigen Functionen durch Auflösung einer Gleichung p^{ten} Grades und ebenso aus jenen durch Auflösung einer ebenso hohen Gleichung die zu $\frac{mP}{p^3}$ gehörigen Functionen u. s. w. abgeleitet, so dass, wenn man das Polygon von p Seiten bereits hat, zur Bestimmung des Polygons von p^λ Seiten notwendig die Auflösung von $\lambda - 1$ Gleichungen p^{ten} Grades erforderlich ist. Obwohl man aber die nachfolgende Theorie auch auf diesen Fall ausdehnen könnte, so würde man doch auf diesem Wege ebenfalls zu so vielen Gleichungen p^{ten} Grades kommen, die sich, wenn p eine Primzahl ist, in keiner Weise auf niedrigere zurückführen lassen. So wird z. B. unten gezeigt werden,

dass sich das Polygon von 17 Seiten geometrisch construieren lässt; aber zur Bestimmung des Polygons von 289 Seiten kann man die Gleichung 17ten Grades in keiner Weise vermeiden.

Gleichungen für die trigonometrischen Functionen der Bogen, welche ein Teil oder Teile der ganzen Peripherie sind; Reduction der trigonometrischen Functionen auf die Wurzeln der Gleichung $x^n - 1 = 0$.

337.

Es ist hinreichend bekannt, dass die trigonometrischen Functionen aller Winkel $\frac{kP}{n}$, wo k unbestimmt alle Zahlen 0, 1, 2, ..., $n-1$ bezeichnet, durch die Wurzeln von Gleichungen n^{ten} Grades ausgedrückt werden, und zwar die Sinus durch die Wurzeln der Gleichung

$$\text{I.}\quad x^n - \frac{1}{4}nx^{n-2} + \frac{1}{16}\frac{n(n-3)}{1\cdot 2}x^{n-4} - \frac{1}{64}\frac{n(n-4)(n-5)}{1\cdot 2\cdot 3}x^{n-6} + \ldots \pm \frac{1}{2^{n-1}}nx = 0,$$

die Cosinus durch die Wurzeln der Gleichung

$$\text{II.}\quad x^n - \frac{1}{4}nx^{n-2} + \frac{1}{16}\frac{n(n-3)}{1\cdot 2}x^{n-4} - \frac{1}{64}\frac{n(n-4)(n-5)}{1\cdot 2\cdot 3}x^{n-6} + \ldots \pm \frac{1}{2^{n-1}}nx - \frac{1}{2^{n-1}} = 0,$$

endlich die Tangenten durch die Wurzeln der Gleichung

$$\text{III.}\quad x^n - \frac{n(n-1)}{1\cdot 2}x^{n-2} + \frac{n(n-1)(n-2)(n-3)}{1\cdot 2\cdot 3\cdot 4}x^{n-4} - \ldots \pm nx = 0.$$

Diese Gleichungen (welche allgemein für jeden ungeraden Wert von n gelten, II aber auch für einen geraden) lassen sich, wenn man $n = 2m+1$ setzt, leicht auf den m^{ten} Grad herabdrücken; nämlich I und III, indem man die linke Seite durch x dividiert und y für x^2 substituiert. Die Gleichung II enthält aber offenbar die Wurzel $x = 1\,(=\cos 0)$, und von den übrigen sind stets je zwei gleich $\left(\cos\frac{P}{n} = \cos\frac{(n-1)P}{n},\ \cos\frac{2P}{n} = \cos\frac{(n-2)P}{n},\ \ldots\right)$; daher ist die linke Seite durch $x-1$ teilbar und der Quotient ein Quadrat; zieht man aus diesem die Quadratwurzel, so reduciert sich die Gleichung II auf die folgende:

$$x^m + \frac{1}{2}x^{m-1} - \frac{1}{4}(m-1)x^{m-2} - \frac{1}{8}(m-2)x^{m-3} + \frac{1}{16}\frac{(m-2)(m-3)}{1\cdot 2}x^{m-4} + \frac{1}{32}\frac{(m-3)(m-4)}{1\cdot 2}x^{m-5} - \ldots = 0,$$

deren Wurzeln die Cosinus der Winkel $\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n}, \ldots, \frac{mP}{n}$ sind. Weitere Reductionen dieser Gleichungen, wenigstens für den Fall, wo n eine Primzahl ist, hatte man bisher nicht.

Indessen ist keine dieser Gleichungen so leicht zu behandeln und für unsern Zweck so geeignet, wie die Gleichung $x^n - 1 = 0$, deren Wurzeln mit den Wurzeln jener bekanntlich auf das Engste zusammenhängen. Schreibt man nämlich der Kürze wegen i für die imaginäre Grösse $\sqrt{-1}$, so werden die Wurzeln der Gleichung $x^n - 1 = 0$ dargestellt durch

$$\cos\frac{kP}{n} + i\sin\frac{kP}{n} = r,$$

wo für k sämtliche Zahlen $0, 1, 2, 3, \ldots, n-1$ zu nehmen sind. Da nun $\frac{1}{r} = \cos\frac{kP}{n} - i\sin\frac{kP}{n}$ ist, so werden somit die Wurzeln der Gleichung I dargestellt durch $\frac{1}{2i}\left(r - \frac{1}{r}\right)$ oder $i\,\frac{1-r^2}{2r}$; die Wurzeln der Gleichung II durch $\frac{1}{2}\left(r + \frac{1}{r}\right) = \frac{1+r^2}{2r}$; endlich die Wurzeln der Gleichung III durch $\frac{i(1-r^2)}{1+r^2}$. Aus diesem Grunde werden wir unsere Untersuchung auf die Betrachtung der Gleichung $x^n - 1 = 0$ gründen, indem wir annehmen, dass n eine ungerade Primzahl sei. Um aber die Reihe der Untersuchungen nicht unterbrechen zu müssen, schicken wir hier den folgenden Hülfssatz voraus.

338.

Aufgabe. Wenn die Gleichung

$$(W)\quad z^m + Az^{m-1} + \cdots = 0$$

gegeben ist, so soll man eine Gleichung (W') finden, deren Wurzeln die λ^{ten} Potenzen der Wurzeln der Gleichung (W) sind, wo λ einen gegebenen positiven ganzen Exponenten bezeichnet.

Auflösung. Bezeichnet man die Wurzeln der Gleichung (W) mit $a, b, c, \ldots$, so müssen die Wurzeln der Gleichung (W') sein: $a^\lambda, b^\lambda, c^\lambda, \ldots$ Nach dem bekannten Newton'schen Satze kann man aus den Coefficienten der Gleichung (W) die Aggregate irgend welcher Potenzen der Wurzeln $a, b, c, \ldots$ finden. Man suche also die Summen

$$a^\lambda + b^\lambda + c^\lambda + \cdots;\ a^{2\lambda} + b^{2\lambda} + c^{2\lambda} \cdots,\ \ldots\ldots,\ \text{bis zu}\ a^{m\lambda} + b^{m\lambda} + c^{m\lambda} + \cdots$$

Aus diesen kann man dann umgekehrt nach demselben Satze die Coefficienten der Gleichung (W') ableiten. — Zugleich geht hieraus hervor, dass, wenn die Coefficienten in (W) rational sind, auch sämtliche Coefficienten in (W') rational werden. Auf anderm Wege kann man zwar auch beweisen, dass, wenn jene ganze Zahlen sind, auch alle diese ganze Zahlen werden; doch halten wir uns bei diesem Satze, der für unsern Zweck nicht so nötig ist, hier nicht auf.

Theorie der Wurzeln der Gleichung $x^n - 1 = 0$ (wo vorausgesetzt wird, dass n eine Primzahl sei). Lässt man die Wurzel 1 weg, so sind die übrigen (Ω) enthalten in der Gleichung $X = x^{n-1} + x^{n-2} + \cdots + x + 1 = 0$.

339.

Die Gleichung $x^n - 1 = 0$ (wo man immer die Voraussetzung hinzudenken muss, dass n eine ungerade Primzahl ist) enthält nur eine einzige reelle Wurzel, $x = 1$; die übrigen $n - 1$ Wurzeln, welche die Gleichung

$$x^{n-1} + x^{n-2} + \cdots + x + 1 = 0$$

umfasst, sind sämtlich imaginär; die Gesamtheit dieser werden wir mit Ω und die Function

$$x^{n-1} + x^{n-2} + \cdots\cdot + x + 1$$

mit X bezeichnen. Wenn daher r irgend eine Wurzel aus Ω ist, so ist $1 = r^n = r^{2n}$ u. s. w., und allgemein $r^{en} = 1$ für jeden ganzen, positiven oder negativen Wert von e; hieraus ist ersichtlich, dass, wenn λ, μ nach dem Modul n congruente ganze Zahlen sind, $r^\lambda = r^\mu$ wird. Sind dagegen λ, μ nach dem Modul n incongruent, so werden r^λ und r^μ ungleich sein; denn in diesem Falle kann man eine ganze Zahl ν derart annehmen, dass $(\lambda - \mu)\nu \equiv 1 \pmod{n}$ wird, woraus $r^{(\lambda-\mu)\nu} = r$ und daher $r^{\lambda-\mu}$ sicher nicht $= 1$ folgt. Ferner ist klar, dass jede Potenz von r ebenfalls Wurzel der Gleichung $x^n - 1 = 0$ ist; daher werden, da die Grössen $1\ (= r^0), r, r^2, \ldots, r^{n-1}$ sämtlich verschieden sind, diese Grössen sämtliche Wurzeln der Gleichung $x^n - 1 = 0$ darstellen und somit die Wurzeln $r, r^2, r^3, \ldots, r^{n-1}$ mit Ω identisch sein. Man schliesst hieraus leicht allgemeiner, dass Ω mit dem Complex der Grössen $r^e, r^{2e}, r^{3e}, \ldots, r^{(n-1)e}$ übereinstimmt, wenn e irgend eine durch n nicht teilbare positive oder negative ganze Zahl ist. Es ist daher:

$$X = (x - r^e)(x - r^{2e})(x - r^{3e}) \ldots (x - r^{(n-1)e}),$$

woraus folgt:

$$r^e + r^{2e} + r^{3e} + \cdots + r^{(n-1)e} = -1 \text{ und } 1 + r^e + r^{2e} + r^{3e} + \cdots + r^{(n-1)e} = 0.$$

Zwei solche Wurzeln wie r und $\frac{1}{r}$ $(= r^{n-1})$ oder allgemein r^e und r^{-e} werden wir reciprok nennen; offenbar wird das Product aus zwei einfachen Factoren $x - r$ und $x - \frac{1}{r}$ reell werden, nämlich $= x^2 - 2x \cos\omega + 1$, so dass der Winkel ω entweder dem Winkel $\frac{P}{n}$ oder irgend einem Vielfachen desselben gleich ist.

340.

Da somit, wenn eine Wurzel aus Ω durch r ausgedrückt wird, sämtliche Wurzeln der Gleichung $x^n - 1 = 0$ durch die Potenzen von r dargestellt werden, so wird das Product, welches aus mehreren Wurzeln dieser Gleichung irgendwie zusammengesetzt ist, durch r^λ dargestellt werden können, so dass λ entweder gleich 0 oder positiv und kleiner als n ist. Bezeichnet man daher mit $\varphi(t, u, v, \ldots)$ eine algebraische rationale ganze Function der Unbestimmten $t, u, v, \ldots$, die man durch eine Summe von Teilen von der Form $ht^\alpha u^\beta v^\gamma \ldots$ ausdrücken kann, so ist klar, dass, wenn für $t, u, v, \ldots$ einige der Wurzeln der Gleichung $x^n - 1 = 0$ substituiert werden, etwa $t = a$, $u = b$, $v = c, \ldots$, die Function $\varphi(a, b, c, \ldots)$ auf die Form

$$A + A'r + A''r^2 + A'''r^3 + \cdots + A^{(n-1)}r^{n-1}$$

gebracht werden kann, so dass die Coefficienten $A, A', \ldots$ (von denen auch einige fehlen und daher gleich 0 werden können) bestimmte Grössen sind und überdies alle diese Coefficienten ganze Zahlen werden, wenn alle bestimmten Coefficienten in $\varphi(t, u, v, \ldots)$ d. h. alle h ganze Zahlen sind. Werden aber darauf für $t, u, v, \ldots$ respective $a^2, b^2, c^2, \ldots$ substituiert, so wird jeder Teil wie $ht^\alpha u^\beta v^\gamma \ldots$, welcher sich vorher auf r^σ reducierte, jetzt $r^{2\sigma}$ werden, woraus man leicht schliesst, dass

$$\varphi(a^2, b^2, c^2, \ldots) = A + A'r^2 + A''r^4 + A'''r^6 + \cdots + A^{(n-1)}r^{2n-2}$$

wird. Ebenso ist allgemein für jeden beliebigen ganzen Wert von λ:

$$\varphi(a^\lambda, b^\lambda, c^\lambda, \ldots) = A + A'r^\lambda + A''r^{2\lambda} + \cdots + A^{(n-1)}r^{(n-1)\lambda},$$

welcher Satz von der grössten Bedeutung ist und die Grundlage der folgenden Untersuchungen bildet. — Hieraus folgt ferner:

$$\varphi(1, 1, 1, \ldots) = \varphi(a^n, b^n, c^n, \ldots) = A + A' + A'' + \cdots + A^{(n-1)}$$

sowie:

$$\varphi(a, b, c, \ldots) + \varphi(a^2, b^2, c^2, \ldots) + \varphi(a^3, b^3, c^3, \ldots) + \cdots + \varphi(a^n, b^n, c^n, \ldots) = nA,$$

so dass also diese Summe immer eine ganze durch n teilbare Zahl ist, wenn sämtliche bestimmten Coefficienten in $\varphi(t, u, v, \ldots)$ ganze Zahlen sind.

Die Function X lässt sich nicht in niedrigere Factoren zerlegen, in denen sämtliche Coefficienten rational sind.

341.

Satz. Wenn die Function X durch die Function niedrigeren Grades

$$P = x^\lambda + Ax^{\lambda-1} + Bx^{\lambda-2} + \cdots + Kx + L$$

teilbar ist, so können die Coefficienten $A, B, \ldots, L$ nicht sämtlich ganze Zahlen sein.

Beweis. Es sei $X = PQ$ und $\mathfrak{P}$ der Complex der Wurzeln der Gleichung $P = 0$, $\mathfrak{Q}$ der Complex der Wurzeln der Gleichung $Q = 0$, so dass Ω aus $\mathfrak{P}$ und $\mathfrak{Q}$ zusammengenommen besteht. Ferner sei $\mathfrak{R}$ der Complex der den Wurzeln $\mathfrak{P}$ reciproken Wurzeln, $\mathfrak{S}$ der Complex der den Wurzeln $\mathfrak{Q}$ reciproken Wurzeln, und es seien die Wurzeln, welche in $\mathfrak{R}$ enthalten sind, Wurzeln der Gleichung $R = 0$, (die, wie man leicht sieht, $x^\lambda + \frac{K}{L}x^{\lambda-1} + \cdots + \frac{A}{L}x + \frac{1}{L} = 0$ ist), und diejenigen, welche in $\mathfrak{S}$ enthalten sind, Wurzeln der Gleichung $S = 0$. Offenbar werden auch die Wurzeln $\mathfrak{R}$ und $\mathfrak{S}$ zusammengenommen den Complex Ω bilden, und es wird $RS = X$ sein. Wir unterscheiden nun vier Fälle.

I. $\mathfrak{P}$ stimmt mit $\mathfrak{R}$ überein und es ist daher $P = R$. In diesem Falle werden offenbar stets je zwei Wurzeln in $\mathfrak{P}$ reciprok sein, und daher ist P das Product aus $\frac{1}{2}\lambda$ doppelten Factoren von der Art wie $x^2 - 2x\cos\omega + 1$; da ein solcher Factor gleich $(x - \cos\omega)^2 + \sin^2\omega$ ist, so sieht man leicht, dass P für jeden beliebigen reellen Wert von x notwendig einen reellen positiven Wert erhält. Es seien die Gleichungen, deren Wurzeln die Quadrate, Kuben, Biquadrate u. s. w. schliesslich die $(n-1)$ ten Potenzen der Wurzeln in $\mathfrak{P}$ sind, $P' = 0$, $P'' = 0$, $P''' = 0, \ldots, P^{(n-1)} = 0$, und es seien die Werte der Functionen $P, P', P'', \ldots, P^{(n-1)}$ welche sie erhalten, wenn man $x = 1$ setzt, respective $p, p', p'', \ldots, p^{(n-1)}$; dann wird nach dem vorher Gesagten p eine positive Grösse sein, und aus ganz ähnlichem Grunde werden auch $p', p'', \ldots$ positiv sein. Da nun p der Wert der Function $(1-t)(1-u)(1-v)\ldots$ ist, welchen sie annimmt, wenn man für $t, u, v\ldots$ die Wurzeln in $\mathfrak{P}$ setzt, p' der Wert derselben Function, wenn man für $t, u, v, \ldots$ die Quadrate jener Wurzeln setzt, u. s. w., und überdies der Wert für $t = 1, u = 1, v = 1, \ldots$ offenbar gleich 0 wird, so ist die Summe $p + p' + p'' + \cdots + p^{(n-1)}$ eine ganze durch n teilbare Zahl. Ausserdem sieht man leicht, dass das Product $P \cdot P' \cdot P'' \ldots = X^\lambda$ und daher $p \cdot p' \cdot p'' \ldots = n^\lambda$ wird.

Wenn nun alle Coefficienten in P rational wären, so würden auch nach Artikel 338 alle Coefficienten in $P', P'', \ldots$ rational werden; nach Artikel 42 aber würden alle diese Coefficienten notwendig ganze Zahlen sein. Hiernach würden auch $p, p', p'', \ldots$ ganze Zahlen sein, und da ihr Produkt gleich n^λ, ihre Anzahl $n - 1$ aber $> \lambda$ ist, so müssten notwendig einige von ihnen (mindestens $n - 1 - \lambda$) gleich 1, die übrigen aber entweder gleich n oder gleich einer Potenz von n sein. Wenn nun aber g von ihnen gleich 1 wären, so würde offenbar die Summe $p + p' + \cdots \equiv g \pmod{n}$ und daher sicher nicht durch n teilbar sein. Daher kann die Annahme nicht stattfinden.

II. Wenn $\mathfrak{P}$ und $\mathfrak{R}$ zwar nicht zusammenfallen, aber doch einige Wurzeln gemeinschaftlich enthalten, so sei $\mathfrak{T}$ der Complex dieser und $T = 0$ die Gleichung, deren Wurzeln sie sind. Dann ist T der grösste gemeinschaftliche Teiler der Functionen P, R (wie aus der Theorie der Gleichungen bekannt ist). Offenbar aber werden in $\mathfrak{T}$ stets je zwei

Wurzeln reciprok sein, und daher können nach dem vorher Bewiesenen nicht sämtliche Coefficienten in T rational sein. Dies würde aber sicher der Fall sein, wenn sämtliche Coefficienten in P und daher auch sämtliche Coefficienten in R rational wären, wie aus der Natur der Operation, durch welche der grösste gemeinschaftliche Teiler gefunden wird, ohne Weiteres sich ergiebt. Daher ist die Annahme absurd.

III. Wenn $\mathfrak{Q}$ und $\mathfrak{S}$ entweder zusammenfallen oder wenigstens gemeinschaftliche Wurzeln enthalten, so können in genau derselben Weise die Coefficienten in Q nicht sämtlich rational sein; sie würden aber rational werden, wenn sämtliche Coefficienten in P rational wären. Daher ist letzteres unmöglich.

IV. Wenn aber weder $\mathfrak{P}$ mit $\mathfrak{R}$ noch $\mathfrak{Q}$ mit $\mathfrak{S}$ irgend eine Wurzel gemeinsam hat, so finden sich notwendig alle Wurzeln $\mathfrak{P}$ in $\mathfrak{S}$ und alle Wurzeln $\mathfrak{Q}$ in $\mathfrak{R}$ vor, so dass $P = S$ und $Q = R$ ist. Daher ist $X = PQ$ das Product aus P in R, d. h.

$$\text{aus } x^\lambda + Ax^{\lambda-1} + \cdots + Kx + L \text{ in } x^\lambda + \frac{K}{L}x^{\lambda-1} + \cdots + \frac{A}{L}x + \frac{1}{L}$$

und hieraus folgt, wenn man $x = 1$ setzt:

$$nL = (1 + A + \cdots + K + L)^2.$$

Wenn nun alle Coefficienten in P rational und daher nach Artikel 42 auch ganz wären, so würde L, welches in dem letzten Coefficienten von X, d. h. in 1 aufgehen müsste, notwendig $= \pm 1$ sein, wonach n eine Quadratzahl wäre. Da dies der Voraussetzung widerspricht, so kann die Annahme nicht bestehen.

Aus diesem Satze geht also hervor, dass, wie auch X in Factoren zerlegt werden möge, ihre Coefficienten wenigstens zum Teil irrational werden und daher nicht anders als durch eine höhere Gleichung bestimmt werden können.

Das Ziel der folgenden Untersuchungen wird angegeben.

342.

Das Ziel der nachfolgenden Untersuchungen, welches kurz anzugeben nicht unnützlich sein wird, geht dahin, X in immer mehr Factoren schrittweise zu zerlegen, und zwar so, dass deren Coefficienten durch Gleichungen von möglichst niedrigem Grade bestimmt werden, bis man auf diese Weise zu einfachen Factoren oder zu den Wurzeln Ω selbst gelangt. Wir werden nämlich zeigen, dass, wenn die Zahl $n - 1$ auf irgend welche Weise in ganzzahlige Factoren $\alpha, \beta, \gamma, \ldots$ (für die man Primzahlen nehmen kann) zerlegt wird, X in α Factoren von $\frac{n-1}{\alpha}$ Dimensionen zerlegt werden kann, deren Coefficienten sich durch

eine Gleichung α^{ten} Grades bestimmen; dass ferner diese einzelnen Factoren wiederum in β andere von $\frac{n-1}{\alpha\beta}$ Dimensionen mit Hülfe einer Gleichung β^{ten} Grades zerlegt werden können u. s. w., so dass, wenn ν die Anzahl der Factoren $\alpha, \beta, \gamma, \ldots$ bezeichnet, die Ermittlung der Wurzeln Ω auf die Auflösung von ν Gleichungen α^{ten}, β^{ten}, γ^{ten}, u. s. w. Grades reduciert wird. So wird man z. B. für $n = 17$, wo $n - 1 = 2 \cdot 2 \cdot 2 \cdot 2$ ist, vier quadratische, für $n = 73$ drei quadratische und zwei kubische Gleichungen auflösen müssen.

Da im Folgenden sehr häufig solche Potenzen der Wurzel r zu betrachten sind, deren Exponenten wiederum Potenzen sind, derartige Ausdrücke aber im Druck nicht ohne Schwierigkeit wiedergegeben werden können, so werden wir uns zur Erleichterung des Druckes im Nachstehenden der folgenden Abkürzung bedienen: Für $r, r^2, r^3, \ldots$ werden wir [1], [2], [3], ... und allgemein für r^λ, wo λ irgend eine ganze Zahl bezeichnet, $[\lambda]$ schreiben. Derartige Ausdrücke sind daher noch nicht völlig bestimmt, sondern werden es erst, sobald für r oder [1] eine bestimmte Wurzel aus Ω genommen wird. Es sind daher allgemein $[\lambda]$, $[\mu]$ gleich oder ungleich, je nachdem λ, μ nach dem Modul n congruent oder incongruent sind. Ferner ist $[0] = 1$; $[\lambda] \cdot [\mu] = [\lambda + \mu]$; $[\lambda]^\nu = [\lambda\nu]$; die Summe $[0] + [\lambda] + [2\lambda] + \cdots + [(n-1)\lambda]$ entweder gleich 0 oder gleich n, je nachdem λ durch n nicht teilbar oder teilbar ist.

Sämtliche Wurzeln Ω werden in gewisse Klassen (Perioden) eingeteilt.

343.

Wenn für den Modul n die Zahl g eine Zahl von jener Art ist, die wir im Abschnitt III primitive Wurzel genannt haben, so sind die $n-1$ Zahlen $1, g, g^2, \ldots, g^{n-2}$ den Zahlen $1, 2, 3, \ldots, n-1$ nach dem Modul n, wenn auch in anderer Reihenfolge, congruent, d. h. jede Zahl der einen Reihe hat in der andern eine congruente Zahl. Hieraus folgt unmittelbar, dass die Wurzeln $[1], [g], [g^2], \ldots, [g^{n-2}]$ mit Ω zusammenfallen, und ganz ebenso werden allgemeiner

$$[\lambda], [\lambda g], [\lambda g^2], \ldots, [\lambda g^{n-2}]$$

mit Ω zusammenfallen, wenn λ irgend eine ganze durch n nicht teilbare Zahl bezeichnet. Ferner sieht man leicht, da $g^{n-1} \equiv 1 \pmod{n}$ ist, dass die beiden Wurzeln $[\lambda g^\mu]$, $[\lambda g^\nu]$ identisch oder verschieden sind, je nachdem μ, ν nach dem Modul $n-1$ congruent oder incongruent sind.

Wenn nun G eine andere primitive Wurzel ist, so werden die Wurzeln $[1], [g], \ldots, [g^{n-2}]$ auch mit $[1], [G], \ldots, [G^{n-2}]$ übereinstimmen, falls man von der Reihenfolge absieht. Aber ausserdem beweist man leicht, dass, wenn e ein Teiler von $n-1$ ist und $n-1 = ef$, $g^e = h$, $G^e = H$ gesetzt wird, auch die f Zahlen $1, h, h^2, \ldots, h^{f-1}$ den folgenden: $1, H,$

$H^2, \ldots, H^{f-1}$ nach n congruent sind (ohne Rücksicht auf die Reihenfolge). Denn nehmen wir $G \equiv g^{\omega}$ (mod. n) an, und ist μ eine willkürliche positive Zahl $< f$ und ν der kleinste Rest von $\mu\omega$ (mod. f), so wird $\nu e \equiv \mu\omega e$ (mod. $n-1$), somit $g^{\nu e} \equiv g^{\mu\omega e} \equiv G^{\mu e}$ (mod. n) oder $H^{\mu} \equiv h^{\nu}$, d. h. zu jeder Zahl der letzteren Reihe 1, H, H^2, ... kommt in der Reihe 1, h, h^2, ... eine congruente vor und umgekehrt. — Hieraus geht hervor, dass die f Wurzeln [1], $[h]$, $[h^2]$, ..., $[h^{f-1}]$ identisch sind mit den folgenden [1], $[H]$, $[H^2]$, ..., $[H^{f-1}]$ und allgemeiner wird man leicht einsehen, dass

$$[\lambda], [\lambda h], [\lambda h^2], \ldots, [\lambda h^{f-1}] \text{ mit } [\lambda], [\lambda H], [\lambda H^2], \ldots, [\lambda H^{f-1}]$$

übereinstimmen. Das Aggregat von f solchen Wurzeln $[\lambda] + [\lambda h] + [\lambda h^2] + \cdots + [\lambda h^{f-1}]$, welches als unabhängig von g zu betrachten ist, da es sich nicht ändert, wenn man für g eine andere primitive Wurzel nimmt, werden wir mit (f, λ) bezeichnen und den Complex derselben Wurzeln die **Periode** (f, λ) nennen, wobei keine Rücksicht auf die Anordnung der Wurzeln genommen wird.*) — Bei der Darstellung einer solchen Periode wird es zweckmässig sein, die einzelnen Wurzeln, aus denen sie besteht, auf den einfachsten Ausdruck zu reducieren, nämlich für die Zahlen λ, λh, λh^2, ... die kleinsten Reste nach dem Modul n zu substituieren, nach deren Grösse, wenn man will, auch die Teile der Periode geordnet werden können.

Beispiel. Für $n = 19$, wo 2 eine primitive Wurzel ist, besteht die Periode (6, 1) aus den Wurzeln [1], [8], [64], [512], [4096], [32768] oder [1], [7], [8], [11], [12], [18]. Ebenso besteht die Periode (6, 2) aus [2], [3], [5], [14], [16], [17]. Die Periode (6, 3) ist identisch mit der vorigen. Die Periode (6, 4) enthält [4], [6], [9], [10], [13], [15].

Verschiedene Sätze über die Perioden der Wurzeln Ω.

344.

In Bezug auf diese Perioden ergeben sich unmittelbar folgende Bemerkungen.

I. Da $\lambda h^f \equiv \lambda$, $\lambda h^{f+1} \equiv \lambda h, \ldots$ (mod. n) ist, so werden offenbar $(f, \lambda h)$, $(f, \lambda h^2)$, ... aus denselben Wurzeln bestehen, aus welchen (f, λ) besteht; bezeichnet also $[\lambda']$ irgend eine Wurzel aus (f, λ), so wird allgemein diese Periode mit (f, λ') vollständig identisch sein. Wenn daher zwei aus gleichviel Wurzeln bestehende Perioden (welche wir **gleichartig** nennen werden) irgend eine Wurzel gemeinsam haben, so sind sie offenbar identisch. Daher ist es nicht möglich, dass zwei Wurzeln in irgend einer Periode

*) Es möge gestattet sein, das Aggregat im Folgenden auch den numerischen Wert der Periode oder einfach Periode zu nennen, wo keine Zweideutigkeit zu befürchten ist.

gleichzeitig enthalten sind, in der andern gleichartigen aber nur eine von ihnen vorkommt; ferner ist klar, dass, wenn zwei Wurzeln $[\lambda]$, $[\lambda']$ zu derselben Periode von f Gliedern gehören, der Wert des Ausdrucks $\frac{\lambda'}{\lambda}$ (mod. n) irgend einer Potenz von h congruent ist, oder dass man setzen kann $\lambda' \equiv \lambda g^{\nu e}$ (mod. n).

II. Ist $f = n - 1$, $e = 1$, so fällt die Periode $(f, 1)$ offenbar mit Ω zusammen; in allen übrigen Fällen aber ist Ω aus den Perioden $(f, 1)$, (f, g), $(f, g^2), \ldots, (f, g^{e-1})$ zusammengesetzt. Diese Perioden sind daher vollständig von einander verschieden, und es ist klar, dass jede andere gleichartige Periode (f, λ) mit irgend einer von diesen zusammenfällt, wofern $[\lambda]$ zu Ω gehört, d. h. wenn λ durch n nicht teilbar ist. Die Periode $(f, 0)$ aber oder (f, kn) ist offenbar aus f Einheiten zusammengesetzt. Ebenso leicht sieht man, dass, wenn λ irgend eine durch n nicht teilbare Zahl ist, auch der Complex der e Perioden (f, λ), $(f, \lambda g)$, $(f, \lambda g^2), \ldots, (f, \lambda g^{e-1})$ mit Ω übereinstimmt. — So besteht z. B. für $n = 19$, $f = 6$ der Complex Ω aus den drei Perioden (6, 1), (6, 2), (6, 4), und auf eine von diesen ist jede andere gleichartige ausser (6, 0) zurückführbar.

III. Wenn $n - 1$ das Product aus drei positiven Zahlen a, b, c ist, so ist offenbar jede Periode von bc Gliedern aus b Perioden von c Gliedern zusammengesetzt, nämlich (bc, λ) aus (c, λ), $(c, \lambda g^a)$, $(c, \lambda g^{2a}), \ldots, (c, \lambda g^{ab-a})$, weshalb diese unter jener enthalten genannt werden. So besteht z. B. für $n = 19$ die Periode (6, 1) aus den dreien (2, 1), (2, 8), (2, 7), deren erste die Wurzeln r, r^{18}, deren zweite die Wurzeln r^8, r^{11} und deren dritte die Wurzeln r^7, r^{12} enthält.

345.

Satz. Es seien (f, λ), (f, μ) zwei gleichartige, identische oder verschiedene, Perioden und es bestehe (f, λ) aus den Wurzeln $[\lambda]$, $[\lambda']$, $[\lambda'']$, ... Dann ist das Product aus (f, λ) und (f, μ) ein Aggregat von f gleichartigen Perioden, nämlich:

$$= (f, \lambda + \mu) + (f, \lambda' + \mu) + (f, \lambda'' + \mu) + \cdots = W.$$

Beweis. Es sei, wie oben, $n - 1 = ef$, g eine primitive Wurzel für den Modul n und $h = g^e$, so dass nach dem Vorhergehenden $(f, \lambda) = (f, \lambda h) = (f, \lambda h^2) = \cdots$ ist. Hiernach ist das gesuchte Product

$$= [\mu] \cdot (f, \lambda) + [\mu h] \cdot (f, \lambda h) + [\mu h^2] \cdot (f, \lambda h^2) + \cdots$$

und daher:

$$\begin{aligned} = & [\lambda + \mu] + [\lambda h + \mu] + \cdots + [\lambda h^{f-1} + \mu] \\ & + [\lambda h + \mu h] + [\lambda h^2 + \mu h] + \cdots + [\lambda h^f + \mu h] \\ & + [\lambda h^2 + \mu h^2] + [\lambda h^3 + \mu h^2] + \cdots + [\lambda h^{f+1} + \mu h^2] \\ & + \cdots . \end{aligned}$$

welcher Ausdruck im ganzen f^2 Wurzeln enthält. Wenn man nun hier die einzelnen Vertikalreihen für sich summiert, so ergiebt sich offenbar:

$$(f,\ \lambda + \mu) + (f,\ \lambda h + \mu) + \cdots + (f,\ \lambda h^{f-1} + \mu),$$

und man sieht leicht, dass dieser Ausdruck mit W übereinstimmt, da die Zahlen $\lambda, \lambda', \lambda'', \ldots$ nach Voraussetzung den Zahlen $\lambda, \lambda h, \lambda h^2, \ldots, \lambda h^{f-1}$ (in welcher Reihenfolge, ist hier gleichgültig) nach dem Modul n congruent und daher auch

die Zahlen $\lambda+\mu, \lambda'+\mu, \lambda''+\mu, \ldots$ den Zahlen $\lambda+\mu, \lambda h+\mu, \lambda h^2+\mu, \ldots, \lambda h^{f-1}+\mu$

congruent sein müssen.

An diesen Satz knüpfen wir einige Zusätze:

I. Bezeichnet k irgend eine ganze Zahl, so ist das Product aus $(f,\ k\lambda)$ und $(f,\ k\mu)$ gleich

$$\big(f,\ k(\lambda + \mu)\big) + \big(f,\ k(\lambda' + \mu)\big) + \big(f,\ k(\lambda'' + \mu)\big) + \cdots$$

II. Da die einzelnen Teile, aus denen W besteht, entweder mit dem Aggregate $(f,\ 0)$, welches gleich f ist, oder mit irgend einem von den folgenden: $(f,\ 1), (f,\ g), (f,\ g^2), \ldots, (f,\ g^{e-1})$ übereinstimmen, so lässt sich W auf die Form bringen:

$$W = af + b(f,\ 1) + b'(f,\ g) + b''(f,\ g^2) + \cdots + b^{(e-1)}(f,\ g^{e-1}),$$

wo die Coefficienten $a, b, b', \ldots$ positive ganze Zahlen (oder einige von ihnen auch 0) sind. Ferner ist klar, dass alsdann das Product aus $(f,\ k\lambda)$ und $(f,\ k\mu)$ wird:

$$af + b(f,\ k) + b'(f,\ kg) + \cdots + b^{(e-1)}(f,\ kg^{e-1}).$$

So wird z. B. für $n = 19$ das Product aus dem Aggregate $(6,\ 1)$ in sich selbst oder das Quadrat dieses Aggregates gleich $(6,\ 2) + (6,\ 8) + (6,\ 9) + (6,\ 12) + (6,\ 13) + (6,\ 19) = 6 + 2(6,\ 1) + (6,\ 2) + 2(6,\ 4)$.

III. Da das Product aus den einzelnen Teilen von W und einer gleichartigen Periode (f, ν) auf eine analoge Form gebracht werden kann, so ist klar, dass auch das Product aus den drei Perioden $(f, \lambda), (f, \mu), (f, \nu)$ durch $cf + d(f,\ 1) + \cdots + d^{(e-1)}(f, g^{e-1})$ dargestellt werden kann, und dass die Coefficienten $c, d, \ldots$ ganze positive Zahlen (oder 0) werden und überdies für jeden beliebigen ganzen Wert von k ist:

$$(f,\ k\lambda) \cdot (f,\ k\mu) \cdot (f,\ k\nu) = cf + d(f,\ k) + d'(f,\ kg) + \cdots$$

Ebenso lässt sich dieser Satz auf Producte von beliebig vielen gleichartigen Perioden ausdehnen, und es ist gleichgültig, ob diese Perioden sämtlich verschieden oder zum Teil oder sämtlich identisch sind.

IV. Hieraus schliesst man, dass, wenn in irgend einer algebraischen rationalen ganzen Function $F = \varphi(t,\ u,\ v,\ \ldots)$ für die Unbestimmten

$t, u, v, \ldots$ respective die gleichartigen Perioden (f, λ), (f, μ), (f, ν), ... substituiert werden, ihr Wert auf die Form

$$A + B(f, 1) + B'(f, g) + B''(f, g^2) + \cdots + B^{(e-1)}(f, g^{e-1})$$

reducierbar ist und die Coefficienten A, B, B', ... sämtlich ganze Zahlen werden, wenn sämtliche bestimmte Coefficienten in F ganze Zahlen sind, und dass, wenn darauf für $t, u, v, \ldots$ respective $(f, k\lambda)$, $(f, k\mu)$, $(f, k\nu)$, ... substituiert werden, der Wert von F die Form annimmt: $A + B(f, k) + B'(f, kg) + \cdots$.

346.

Satz. Nimmt man an, dass λ eine durch n nicht teilbare Zahl sei, und schreibt man der Kürze wegen p für (f, λ), so lässt sich jede andere gleichartige Periode (f, μ), wo auch μ durch n nicht teilbar angenommen wird, auf folgende Form reducieren

$$\alpha + \beta p + \gamma p^2 + \cdots + \vartheta p^{e-1},$$

so dass die Coefficienten α, β, ... bestimmte rationale Grössen sind.

Beweis. Man bezeichne zur Abkürzung die Perioden $(f, \lambda g)$, $(f, \lambda g^2)$, $(f, \lambda g^3)$, ..., $(f, \lambda g^{e-1})$, deren Anzahl $e-1$ ist, und mit deren einer (f, μ) notwendig übereinstimmt, mit p', p'', p''', ... Dann hat man also sofort die Gleichung:

$$\text{(I)} \qquad 0 = 1 + p + p' + p'' + p''' + \cdots$$

Entwickelt man aber nach den Regeln des vorigen Artikels die Werte der Potenzen von p bis zur $(e-1)$ten, so erhält man noch $e-2$ andere von der Form:

$$\begin{array}{ll}\text{(II)} & 0 = p^2 + A + ap + a'p' + a''p'' + a'''p''' + \cdots \\ \text{(III)} & 0 = p^3 + B + bp + b'p' + b''p'' + b'''p''' + \cdots \\ \text{(IV)} & 0 = p^4 + C + cp + c'p' + c''p'' + c'''p''' + \cdots \\ & \ldots\ldots\ldots\ldots\ldots\ldots, \end{array}$$

wo sämtliche Coefficienten A, a, a', ..., B, b, b', ..., ... ganze Zahlen und, was wohl zu beachten ist und aus dem vorigen Artikel unmittelbar folgt, von λ gänzlich unabhängig sind; d. h. dieselben Gleichungen gelten auch noch, welchen andern Wert man auch λ beilegen möge; diese Bemerkung erstreckt sich offenhar auch auf die Gleichung (I), wenn nur λ durch n nicht teilbar angenommen wird. — Wir nehmen $(f, \mu) = p'$ an, denn man sieht sehr leicht, dass, wenn (f, μ) mit irgend einer andern Periode aus p'', p''', ... übereinstimmt, den folgenden ganz analoge Schlüsse angewendet werden können. Da die Anzahl der Gleichungen (I), (II), (III), ... gleich $e-1$ ist, so lassen sich die Grössen p'', p''', ..., deren Anzahl gleich $e-2$ ist, nach bekannten Methoden daraus eliminieren, so dass sich eine von ihnen freie Gleichung wie

$$(Z) \quad 0 = \mathfrak{A} + \mathfrak{B}p + \mathfrak{C}p^2 + \cdots + \mathfrak{M}p^{e-1} + \mathfrak{N}p'$$

ergiebt, und zwar kann dies so geschehen, dass sämtliche Coefficienten $\mathfrak{A}$, $\mathfrak{B}$, ..., $\mathfrak{N}$ ganze Zahlen und sicher nicht alle gleich Null sind. Wenn nun hier $\mathfrak{N}$ nicht gleich Null ist, so geht daraus sofort hervor, dass p' dadurch in der Weise, wie der Satz es behauptet, bestimmt wird. Wir haben also nur noch nachzuweisen, dass $\mathfrak{N}$ nicht gleich 0 werden kann.

Nimmt man an, dass $\mathfrak{N} = 0$ sei, so wird die Gleichung (Z): $\mathfrak{M}p^{e-1} + \cdots + \mathfrak{B}p + \mathfrak{A} = 0$, und dieser können, da sie den $(e-1)^{\text{ten}}$ Grad sicher nicht übersteigen kann, nicht mehr als $e-1$ verschiedene Werte von p genügen. Da aber die Gleichungen, aus denen (Z) abgeleitet ist, von λ unabhängig sind, so ist klar, dass auch (Z) von λ nicht abhängt, also stattfindet, welche ganze durch n nicht teilbare Zahl man auch für λ nehmen möge. Daher wird die Gleichung (Z) befriedigt werden, welchem von den Aggregaten $(f, 1)$, (f, g), (f, g^2), ..., $(f.g^{e-1})$ man auch p gleichsetzen möge, woraus von selbst folgt, dass diese Aggregate nicht sämtlich ungleich sein können, sondern mindestens zwei unter ihnen gleich sein müssen. Es möge das eine von zwei solchen gleichen Aggregaten die Wurzeln $[\zeta]$, $[\zeta']$, $[\zeta'']$, ..., das andere die Wurzeln $[\eta]$, $[\eta']$, $[\eta'']$, ... enthalten, und man nehme an (was erlaubt ist), dass sämtliche Zahlen ζ, ζ', ζ'', ..., η, η', η'', ... positiv und kleiner als n seien; offenbar werden sie auch sämtlich verschieden und keine von ihnen gleich 0 sein. Bezeichnet man die Function

$$x^{\zeta} + x^{\zeta'} + x^{\zeta''} + \cdots - x^{\eta} - x^{\eta'} - x^{\eta''} - \cdots,$$

deren höchstes Glied nicht über x^{n-1} hinaus liegen kann, mit Y, so wird offenbar $Y = 0$ für $x = [1]$; demnach enthält Y den Factor $x - [1]$, und zwar wird sie diesen mit der Function, welche wir im Vorigen mit X bezeichnet haben, gemeinsam haben. Dass dies aber absurd ist, lässt sich leicht zeigen. Denn wenn Y mit X irgend einen Factor gemeinschaftlich hätte, so würde der grösste gemeinschaftliche Teiler der Functionen X, Y (dass derselbe sicher nicht bis zu $n-1$ Dimensionen ansteigen kann, geht schon daraus hervor, dass Y durch x teilbar ist) lauter rationale Coefficienten haben, wie aus der Natur der Operationen, durch welche man den grössten gemeinschaftlichen Teiler zweier Functionen, deren Coefficienten sämtlich rational sind, ermittelt, ohne weiteres sich ergiebt. Im Artikel 341 haben wir aber gezeigt, dass X keinen Factor von weniger als $n-1$ Dimensionen, dessen Coefficienten sämtlich rational sind, enthalten kann. Daher kann die Annahme, dass $\mathfrak{N} = 0$ sei, nicht richtig sein.

Beispiel. Für $n = 19$, $f = 6$ wird $p^2 = 6 + 2p + p' + 2p''$; hieraus und aus $0 = 1 + p + p' + p''$ leitet man her: $p' = 4 - p^2$, $p'' = -5 - p + p^2$. Mithin:

$$(6, 2) = 4 - (6, 1)^2, \quad (6, 4) = -5 - (6, 1) + (6, 1)^2$$
$$(6, 4) = 4 - (6, 2)^2, \quad (6, 1) = -5 - (6, 2) + (6, 2)^2$$
$$(6, 1) = 4 - (6, 4)^2, \quad (6, 2) = -5 - (6, 4) + (6, 4)^2.$$

347.

Satz. Ist $F = \varphi(t, u, v, \ldots)$ eine symmetrische (invariable)*) algebraische rationale ganze Function der f Unbestimmten $t, u, v, \ldots$, und substituiert man für diese die f in der Periode (f, λ) enthaltenen Wurzeln, so lässt sich der Wert von F nach den Vorschriften des Artikels 340 auf die Form

$$A + A'[1] + A''[2] + \cdots = W$$

bringen. Die Wurzeln, welche in diesem Ausdrucke zu einer und derselben Periode von f Gliedern gehören, werden dann gleiche Coefficienten haben.

Beweis. Es seien $[p]$, $[q]$ zwei zu einer und derselben Periode gehörige Wurzeln, und man nehme p, q positiv und kleiner als n an; dann soll bewiesen werden, dass $[p]$ und $[q]$ in W denselben Coefficienten haben. Es sei $q \equiv pg^{\nu e}$ (mod. n); es seien ferner die in (f, λ) enthaltenen Wurzeln $[\lambda]$, $[\lambda']$, $[\lambda'']$, ..., wo die Zahlen $\lambda, \lambda', \lambda'', \ldots$ positiv und kleiner als n vorausgesetzt werden; endlich seien die kleinsten positiven Reste der Zahlen $\lambda g^{\nu e}, \lambda' g^{\nu e}, \lambda'' g^{\nu e}, \ldots$ nach dem Modul n respective $\mu, \mu', \mu'', \ldots$ welche offenbar mit den Zahlen $\lambda, \lambda', \lambda'', \ldots$, wenn auch in anderer Reihenfolge identisch sind. Nun geht aus Artikel 340 hervor, dass

$$\varphi([\lambda g^{\nu e}], [\lambda' g^{\nu e}], [\lambda'' g^{\nu e}], \ldots) = (I)$$

die Form annimmt:

$$A + A'[g^{\nu e}] + A''[2g^{\nu e}] + \cdots \quad \text{oder} \quad A + A'[\vartheta] + A''[\vartheta''] + \cdots = (W'),$$

wenn $\vartheta, \vartheta', \vartheta'', \ldots$ die kleinsten Reste der Zahlen $g^{\nu e}, 2g^{\nu e}, \ldots$ nach dem Modul n bezeichnen, woraus ersichtlich ist, dass $[q]$ in $[W']$ denselben Coefficienten hat, wie $[p]$ in $[W]$. Man sieht aber leicht, dass sich aus der Entwicklung des Ausdruckes (I) dasselbe Resultat ergiebt, wie aus der Entwicklung von $\varphi([\mu], [\mu'], [\mu''], \ldots)$, da $\mu \equiv \lambda g^{\nu e}, \mu' \equiv \lambda' g^{\nu e}, \ldots$ (mod. n) ist; dieser Ausdruck aber ergiebt wieder dasselbe Resultat wie $\varphi([\lambda], [\lambda'], [\lambda''], \ldots)$, da die Zahlen $\mu, \mu', \mu'', \ldots$ von $\lambda, \lambda', \lambda'', \ldots$ nur in der Reihenfolge abweichen, und es auf diese bei symmetrischen Functionen nicht ankommt. Hieraus schliesst man, dass W' mit W völlig identisch ist, so dass also die Wurzel $[q]$ in W denselben Coefficienten hat wie $[p]$.

Hiernach kann W offenbar auf die Form

$$A + a\,(f, 1) + a'(f, g) + a''(f, g^2) + \cdots + a^{(e-1)}(f, g^{e-1})$$

gebracht werden, so dass die Coefficienten $A, a, \ldots, a^{(e-1)}$ bestimmte Grössen sind, die überdies ganze Zahlen sein werden, wenn sämtliche rationalen

*) Symmetrische (invariabiles) Functionen werden bekanntlich diejenigen Functionen genannt, welche alle Unbestimmten in derselben Weise enthalten, oder deutlicher, die sich nicht ändern, wie man auch die Unbestimmten unter sich vertauschen möge; solche Functionen sind z. B. die Summe aller Unbestimmten, das Product aus allen, die Summe der Producte aus je zweien u. s. w.

Coefffcienten in F ganze Zahlen sind. — So lässt sich z. B., wenn $n = 19$, $f = 6$, $\lambda = 1$ ist, und φ das Aggregat der Producte aus je zwei Unbestimmten bezeichnet, der Wert von φ auf die Form bringen: $3 + (6, 1) + (6, 4)$.

Ferner sieht man leicht, dass, wenn man darauf für $t, u, v, \ldots$ die Wurzeln aus einer andern Periode $(f, k\lambda)$ substituiert, der Wert von F gleich

$$A + a(f, k) + a'(f, kg) + a''(f, kg^2) + \cdots$$

wird.

348.

Da in jeder Gleichung

$$x^f - \alpha x^{f-1} + \beta x^{f-2} - \gamma x^{f-3} + \cdots = 0$$

die Coefficienten $\alpha, \beta, \gamma, \ldots$ symmetrische Functionen der Wurzeln sind, nämlich α die Summe aller Wurzeln, β die Summe der Produkte aus je zweien, γ die Summe der Produkte aus je dreien u. s. w., so ist in der Gleichung, deren Wurzeln die in der Periode (f, λ) enthaltenen Wurzeln sind, der erste Coefficient gleich (f, λ), während jeder der übrigen auf die Form

$$A + a(f, 1) + a'(f, g) + \cdots + a^{(e-1)}(f, g^{e-1}),$$

wo $A, a, a', \ldots$ sämtlich ganze Zahlen sind, gebracht werden kann; und ausserdem ist klar, dass die Gleichung, deren Wurzeln die in irgend einer andern Periode $(f, k\lambda)$ enthaltenen Wurzeln sind, aus jener entsteht, wenn man in den einzelnen Coefficienten (f, k) für $(f, 1)$, (f, kg) für (f, g) und allgemein (f, kp) für (f, p) substituiert. Auf diese Weise kann man daher e Gleichungen $z=0$, $z'=0$, $z''=0, \ldots$ angeben, deren Wurzeln die in $(f, 1)$, (f, g), $(f, g^2), \ldots$ enthaltenen Wurzeln sind, sobald die e Aggregate $(f, 1)$, (f, g), $(f, g^2), \ldots$ bekannt sind, oder vielmehr, sobald irgend eins derselben gefunden ist, da nach Artikel 346 aus einem einzigen alle übrigen rational abgeleitet werden können. Auf diese Weise erhält man zugleich die Zerlegung der Function X in e Factoren von f Dimensionen; denn das Produkt aus den Functionen $z, z', z'', \ldots$ ist offenbar gleich X.

Beispiel. Für $n = 19$ ist die Summe aller Wurzeln in der Periode (6, 1) gleich $(6, 1) = \alpha$; die Summe der Producte aus je zweien wird gleich $3 + (6,1) + (6, 4) = \beta$; analog findet man die Summe der Produkte aus je dreien gleich $2 + 2(6, 1) + (6, 2) = \gamma$, die Summe der Producte aus je vieren gleich $3 + (6, 1) + (6, 4) = \delta$, die Summe der Produkte aus je fünfen gleich $(6, 1) = \varepsilon$, das Produkt aus allen gleich 1. Somit umfasst die Gleichung

$$z = x^6 - \alpha x^5 + \beta x^4 - \gamma x^3 + \delta x^2 - \varepsilon x + 1 = 0$$

sämtliche in (6, 1) enthaltene Wurzeln. Werden nun in den Coefficienten $\alpha, \beta, \gamma, \ldots$ für (6, 1), (6, 2), (6, 4) respective (6, 2), (6, 4), (6, 1) substituiert, so geht die Gleichung $z'=0$ hervor, welche die in (6, 2) enthaltenen Wurzeln umfasst, und wenn dieselbe Vertauschung hier nochmals angewendet wird, erhält man die Gleichung $z''= 0$, welche die in (6, 4) enthaltenen Wurzeln umfasst, und das Product $zz'z''$ ist gleich X.

349.

Meistens ist es bequemer, besonders wenn f eine grosse Zahl ist, die Coefficienten $\alpha, \beta, \gamma, \ldots$ nach dem Newton'schen Satze aus den Potenzsummen der Wurzeln abzuleiten. Es ist nämlich ohne Weiteres klar, dass die Summe der Quadrate der in (f, λ) enthaltenen Wurzeln gleich $(f, 2\lambda)$, die Summe der Kuben gleich $(f, 3\lambda)$ u. s. w. ist. Schreibt man daher der Kürze wegen für (f, λ), $(f, 2\lambda)$, $(f, 3\lambda), \ldots$ respective $q, q', q'', \ldots$, so ist:

$$\alpha = q, \quad 2\beta = \alpha q - q', \quad 3\gamma = \beta q - \alpha q' + q'', \ldots,$$

wobei die Producte aus zwei Perioden nach Artikel 345 sogleich in Summen von Perioden verwandelt werden müssen. So werden in unserm Beispiel, wenn man für (6, 1), (6, 2), (6, 4) respective p, p', p'' schreibt, die Grössen $q, q', q'', q''', q'''', q'''''$ bezüglich gleich p, p', p', p'', p', p''; demnach:

$$\begin{aligned}
\alpha &= p,\\
2\beta &= p^2 - pp' = 6 + 2p + 2p''\\
3\gamma &= (3 + p + p'')p - pp' + p' = 6 + 6p + 3p'\\
4\delta &= (2 + 2p + p')p - (3 + p + p'')p' + pp' - p'' = 12 + 4p + 4p''
\end{aligned}$$

u. s. w.

Übrigens braucht man nur die Hälfte der Coefficienten auf diese Weise zu berechnen; denn es ist nicht schwer zu beweisen, dass die letzten in umgekehrter Reihenfolge den ersten gleich sind, nämlich der letzte gleich 1, der vorletzte gleich α, der vorvorletzte gleich β, u. s. w., oder aus eben diesen respective hervorgehen, wenn man für $(f, 1)$, $(f, g) \ldots$ setzt: $(f, -1)$, $(f, -g), \ldots$ oder $(f, n-1)$, $(f, n-g), \ldots$ Der erste Fall findet statt, wenn f gerade, der zweite, wenn f ungerade ist; der letzte Coefficient wird aber immer gleich 1. Der Grund hiervon beruht auf dem Satze in Artikel 79; doch halten wir uns der Kürze wegen bei diesem Gegenstande nicht auf.

350.

Satz. Es sei $n-1$ das Product aus den drei positiven Zahlen α, β, γ; es möge ferner die Periode $(\beta\gamma, \lambda)$, welche $\beta\gamma$ Glieder besitzt, aus β kleineren Perioden von γ Gliedern, nämlich (γ, λ), (γ, λ'), $(\gamma, \lambda''), \ldots$ bestehen, und es werde angenommen, dass, wenn in einer Function von β Unbestimmten von gleicher Beschaffenheit wie die im Artikel 347, nämlich in $F = \varphi(t, u, v, \ldots)$ für die Unbestimmten $t, u, v, \ldots$ die Aggregate (γ, λ), (γ, λ'), $(\gamma, \lambda''), \ldots$ respective substituiert werden, der Wert derselben nach den Regeln im Artikel 345 IV reduciert werde auf

$$A + a(\gamma, 1) + a'(\gamma, g) + \cdots + a^{(\zeta)}(\gamma, g^{\alpha\beta-\alpha}) + \cdots + a^{(\theta)}(\gamma, g^{\alpha\beta-1}) = W$$

Dann behaupte ich, dass, wenn F eine symmetrische Function ist, diejenigen Perioden in W, welche in derselben Periode von $\beta\gamma$ Gliedern enthalten sind, d. h. allgemein Perioden wie

(γ, g^{μ}) und $(\gamma, g^{\alpha\nu+\mu})$, wo ν irgend eine ganze Zahl bezeichnet, dieselben Coefficienten haben werden.

Beweis. Da die Periode $(\beta\gamma, \lambda g^{\alpha})$ identisch ist mit $(\beta\gamma, \lambda)$, so werden die kleineren Perioden, $(\gamma, \lambda g^{\alpha})$, $(\gamma, \lambda' g^{\alpha})$, $(\gamma, \lambda'' g^{\alpha})$, ..., aus denen die erstere offenbar besteht, notwendig mit denjenigen übereinstimmen, aus denen die letztere besteht, allerdings in anderer Reihenfolge. Wenn man also annimmt, dass, nachdem jene für t, u, v, ... respective substituiert sind, F in W' übergehe, so wird W' mit W zusammenfallen. Nach Artikel 347 aber ist:

$$W' = A + a(\gamma, g^{\alpha}) + a'(\gamma, g^{\alpha+1}) + \cdots + a^{(\zeta)}(\gamma, g^{\alpha\beta}) + \cdots + a^{(\vartheta)}(\gamma, g^{\alpha\beta+\alpha-1})$$
$$= A + a(\gamma, g^{\alpha}) + a'(\gamma, g^{\alpha+1}) + \cdots + a^{(\zeta)}(\gamma, 1) + \cdots + a^{(\vartheta)}(\gamma, g^{\alpha-1}).$$

Mithin muss, da dieser Ausdruck mit W übereinstimmen soll, der erste, zweite, dritte, u. s. w. Coefficient in W (von a an gerechnet) notwendig mit dem $(\alpha+1)$ten, $(\alpha+2)$ten, $(\alpha+3)$ten, u. s. w. übereinstimmen, woraus man leicht schliesst, dass allgemein die Coefficienten der Perioden (γ, g^{μ}), $(\gamma, g^{\alpha+\mu})$, $(\gamma, g^{2\alpha+\mu})$, ..., $(\gamma, g^{\nu\alpha+\mu})$, welche an $(\mu+1)$ter, $(\alpha+\mu+1)$ter, $(2\alpha+\mu+1)$ter, ..., $(\nu\alpha+\mu+1)$ter Stelle stehen, unter sich übereinstimmen müssen. W. z. b. w.

Hieraus geht hervor, dass W reduciert werden kann auf die Form:

$$A + a(\beta\gamma, 1) + a'(\beta\gamma, g) + \cdots + a^{(\alpha-1)}(\beta\gamma, g^{\alpha-1}),$$

in welcher sämtliche Coefficienten A, a, ... ganze Zahlen sein werden, wenn sämtliche bestimmten Coefficienten in F ganze Zahlen sind. Ferner sieht man leicht, dass, wenn nachher für die Unbestimmten in F die β Perioden von γ Gliedern, welche in einer andern Periode von $\beta\gamma$ Gliedern, etwa in $(\beta\gamma, \lambda k)$, enthalten sind und die offenbar $(\gamma, \lambda k)$, $(\gamma, \lambda' k)$, $(\gamma, \lambda'' k)$, ... sind, substituiert werden, der daraus hervorgehende Wert lautet: $A + a(\beta\gamma, k) + a'(\beta\gamma, gk) + \cdots + a^{(\alpha-1)}(\beta\gamma, g^{\alpha-1}k)$.

Ferner ist klar, dass der Satz auch auf den Fall ausgedehnt werden kann, wo $\alpha = 1$ oder $\beta\gamma = n - 1$ ist; hier sind nämlich sämtliche Coefficienten in W gleich und daher reduciert sich W auf die Form $A + a(\beta\gamma, 1)$.

351.

Behält man also sämtliche Bezeichnungen des vorigen Artikels bei, so ist klar, dass die einzelnen Coefficienten der Gleichung, deren Wurzeln die β Aggregate (γ, λ), (γ, λ'), (γ, λ''), ... sind, auf eine Form wie

$$A + a(\beta\gamma, 1) + a'(\beta\gamma, g) + \cdots + a^{(\alpha-1)}(\beta\gamma, g^{\alpha-1})$$

reduciert werden können, und dass die Zahlen A, a, ... sämtlich ganze Zahlen werden, dass aber die Gleichung, deren Wurzeln die β in einer andern Periode $(\beta\gamma, k\lambda)$ enthaltenen Periode von γ Gliedern sind, aus jener abgeleitet wird, wenn überall in den Coefficienten für jede beliebige Periode $(\beta\gamma, \mu)$ substituiert wird $(\beta\gamma, k\mu)$. Ist also $\alpha = 1$, so werden sämtliche β

Perioden von γ Gliedern bestimmt durch eine Gleichung β ten Grades, deren einzelne Coefficienten sich auf die Form $A + a\,(\beta\gamma, 1)$ reducieren und daher bekannte Grössen sind, da $(\beta\gamma, 1) = (n-1, 1) = -1$ ist. Ist aber $\alpha > 1$, so sind die Coefficienten der Gleichung, deren Wurzeln sämtliche in irgend einer gegebenen Periode von $\beta\gamma$ Gliedern enthaltenen Perioden von γ Gliedern sind, bekannte Grössen, sobald die numerischen Werte aller α Perioden von $\beta\gamma$ Gliedern bekannt sind. — Übrigens lässt sich die Berechnung der Coefficienten dieser Gleichungen häufig, besonders wenn β nicht sehr klein ist, bequemer anstellen, wenn man zunächst die Potenzsummen der Wurzeln ermittelt und sodann aus diesen, ebenso wie oben im Artikel 349 nach dem Newton'schen Satze die Coefficienten ableitet.

Beispiel I. Man sucht für $n = 19$ die Gleichung, deren Wurzeln die Aggregate (6, 1), (6, 2), (6, 4) sind. Bezeichnet man diese Wurzeln mit p, p', p'' respective und die gesuchte Gleichung mit

$$x^3 - Ax^2 + Bx - C = 0,$$

so folgt:

$$A = p + p' + p'', \quad B = pp' + pp'' + p'p'', \quad C = pp'p''.$$

Hiernach ist:

$$A = (18, 1) = -1;$$

ferner hat man:

$$pp' = p + 2p' + 3p'', \quad pp'' = 2p + 3p' + p'', \quad p'p'' = 3p + p' + 2p'',$$

daher:

$$B = 6\,(p + p' + p'') = 6(18,\ 1) = -6;$$

endlich wird

$$C = (p + 2p' + 3p'')\,p'' = 3\,(6, 0) + 11\,(p + p' + p'') = 18 - 11 = 7.$$

Daher ist die gesuchte Gleichung:

$$x^3 + x^2 - 6x - 7 = 0.$$

Bedient man sich der andern Methode, so hat man:

$$p + p' + p'' = -1$$

$$p^2 = 6 + 2p + p' + 2p'', \; p'^2 = 6 + 2p' + p'' + 2p, \; p''^2 = 6 + 2p'' + p + 2p',$$

daher:

$$p^2 + p'^2 + p''^2 = 18 + 5(p + p' + p'') = 13$$

und ebenso:

$$p^3 + p'^3 + p''^3 = 36 + 34(p + p' + p'') = 2.$$

Hieraus leitet man nach dem Newton'schen Gesetze dieselbe Gleichung ab, wie vorher.

II. Gesucht wird für $n = 19$ die Gleichung, deren Wurzeln die Aggregate (2, 1), (2, 7), (2, 8) sind. Bezeichnet man diese respective mit q, q', q'', so findet man:

$$q + q' + q'' = (6, 1), \quad qq' + qq'' + q'q'' = (6, 1) + (6, 4), \quad qq'q'' = 2 + (6, 2),$$

daher ist mit Beibehaltung der Bezeichnungen des vorigen Artikels die gesuchte Gleichung:

$$x^3 - px^2 + (p + p'')x - 2 - p' = 0.$$

Die Gleichung, deren Wurzeln die unter (6, 2) enthaltenen Aggregate (2, 2), (2, 3), (2, 5) sind, geht aus der vorstehenden hervor, wenn man für p, p', p'' respective p', p'', p substituiert, und führt man dieselbe Substitution nochmals aus, so entsteht die Gleichung, deren Wurzeln die unter (6, 4) enthaltenen Aggregate (2, 4), (2, 6), (2, 9) sind.

Auf die vorstehenden Untersuchungen wird die Lösung der Gleichung $X = 0$ gegründet.

352.

Die vorstehenden Sätze mit den daran geknüpften Folgerungen enthalten die hauptsächlichsten Punkte der ganzen Theorie, und die Methode, die Werte der Wurzeln Ω zu finden, kann nunmehr mit wenig Worten dargelegt werden.

Vor allem muss man eine Zahl g annehmen, welche für den Modul n primitive Wurzel ist, und die kleinsten Reste der Potenzen von g bis zu g^{n-2} nach dem Modul n ermitteln. Man zerlege $n - 1$ in Factoren und zwar, wenn man das Problem auf Gleichungen von möglichst niedrigem Grade reducieren will, in Primzahlen; dieselbe seien (in ganz willkürlicher Reihenfolge) $\alpha, \beta, \gamma, \ldots, \zeta$, und man setze:

$$\frac{n-1}{\alpha} = \beta\gamma \ldots \zeta = a, \quad \frac{n-1}{\alpha\beta} = \gamma \ldots \zeta = b, \ldots.$$

Man teile sämtliche Wurzeln Ω in α Perioden von a Gliedern, jede einzelne von diesen wieder in β Perioden von b Gliedern, jede einzelne von diesen wiederum in γ Perioden, u. s. w. Man suche nach dem vorigen Artikel die Gleichung α^{ten} Grades (A), deren Wurzeln jene α Aggregate von a Gliedern sind; die Werte dieser letzteren werden somit nach Auflösung dieser Gleichung bekannt sein.

Hier entsteht aber eine Schwierigkeit, da es ungewiss erscheint, welcher Wurzel der Gleichung (A) ein jedes Aggregat gleichzusetzen ist, d. h. welche Wurzel mit $(a, 1)$, welche mit $(a, g), \ldots$ bezeichnet werden muss. Diesem Übelstande kann man in folgender Weise abhelfen. Mit $(a, 1)$ kann man jede Wurzel der Gleichung (A) bezeichnen; denn da jede Wurzel dieser Gleichung ein Aggregat von a Wurzeln aus Ω ist und es ganz willkürlich ist, welche Wurzel aus Ω mit [1] bezeichnet wird, so darf man offenbar annehmen, dass irgend eine von denjenigen Wurzeln, aus welchen irgend eine gegebene Wurzel der Gleichung (A) besteht, durch [1] dargestellt werde, wonach jene Wurzel der Gleichung (A) $(a, 1)$ wird. Die Wurzel [1] wird

hierdurch aber noch nicht vollständig bestimmt, sondern es bleibt noch ganz willkürlich oder unbestimmt, welche Wurzel von denjenigen, die $(a, 1)$ bilden, wir für [1] nehmen wollen. Sobald aber $(a, 1)$ bestimmt ist, so können auch alle übrigen Aggregate von a Gliedern rational daraus abgeleitet werden (Artikel 346). Hieraus geht zugleich hervor, dass man nur eine einzige Wurzel durch Auflösung dieser Gleichung zu ermitteln braucht. — Man kann zu diesem Zwecke auch die folgende weniger directe Methode anwenden. Man nehme für [1] eine bestimmte Wurzel, d. h. man setze $[1] = \cos\frac{kP}{n} + i\sin\frac{kP}{n}$, wo die ganze Zahl k willkürlich gewählt ist, jedoch so, dass sie durch n nicht teilbar ist; dann werden auch [2], [3], ... bestimmte Wurzeln andeuten, daher denn auch die Aggregate $(a, 1)$, (a, g), ... bestimmte Grössen bezeichnen werden. Hat man diese aus den Sinustafeln auf nur wenige Stellen berechnet, nämlich soweit, dass man entscheiden kann, welche grösser, welche kleiner sind, so kann kein Zweifel mehr übrig sein, durch welche Bezeichnungen die einzelnen Wurzeln der Gleichung (A) zu unterscheiden sind.

Nachdem auf diese Weise sämtliche α Aggregate von a Gliedern gefunden sind, suche man nach dem vorigen Artikel die Gleichung β^{ten} Grades (B), deren Wurzeln die β Aggregate von b Gliedern sind, welche in $(a, 1)$ vorkommen; die Coefficienten dieser Gleichung werden sämtlich bekannt sein. Da es noch willkürlich ist, welche von den $a = \beta b$ unter $(a, 1)$ enthaltenen Wurzeln mit [1] bezeichnet wird, so kann man jede beliebige gegebene Wurzel der Gleichung (B) durch $(b, 1)$ darstellen, da man offenbar annehmen darf, dass irgend eine der b Wurzeln, aus denen sie zusammengesetzt ist, mit [1] bezeichnet werde. Man ermittle also durch Auflösung der Gleichung (B) nur irgend eine Wurzel dieser Gleichung, setze sie gleich $(b, 1)$ und leite daraus nach Artikel 346 alle übrigen Aggregate von b Gliedern ab. Auf diese Weise erhalten wir zugleich eine Probe für die Rechnung, da immer diejenigen Aggregate von b Gliedern, welche zu denselben Perioden von a Gliedern gehören, bekannte Summen ergeben müssen. — In manchen Fällen würde es ebenso einfach sein, $\alpha - 1$ andere Gleichungen β^{ten} Grades abzuleiten, deren Wurzeln respective die einzelnen β Aggregate von b Gliedern sind, die in den übrigen Perioden von a Gliedern (a, g), (a, g^2), ... enthalten sind, und sämtliche Wurzeln sowohl dieser Gleichungen als auch der Gleichung (B) durch Auflösung zu suchen; dann aber müsste man ebenso wie oben mit Hülfe der Sinustafel entscheiden, welchen Perioden von b Gliedern die einzelnen auf diese Weise sich ergebenden Wurzeln gleich gesetzt werden müssen. Übrigens können für diese Entscheidung noch viele andere Kunstgriffe angewendet werden, die wir an dieser Stelle nicht vollständig darlegen können; nur einen für den Fall, wo $\beta = 2$ ist, der besonders nützlich ist und kürzer durch Beispiele als durch theoretische Betrachtungen klargemacht werden kann, wird man in den folgenden Beispielen kennen lernen.

Nachdem auf diese Weise die Werte aller $\alpha\beta$ Aggregate von b Gliedern gefunden sind, können auf ganz ähnliche Weise daraus mittelst Gleichungen vom γ^{ten} Grade sämtliche $\alpha\beta\gamma$ Aggregate von c Gliedern bestimmt werden. Nämlich entweder wird man eine einzige Gleichung γ^{ten} Grades, deren Wurzeln die γ in $(b, 1)$ enthaltenen Aggregate von c Gliedern sind, nach Artikel 350 ermitteln, durch Auflösung derselben irgend eine Wurzel suchen und gleich $(c, 1)$ setzen und schliesslich hieraus nach Artikel 346 alle übrigen ähnlichen Aggregate ableiten müssen, oder man muss auf gleiche Weise überhaupt $\alpha\beta$ Gleichungen γ^{ten} Grades aufstellen, deren Wurzeln respective die γ Aggregate von c Gliedern sind, die in den einzelnen Perioden von b Gliedern enthalten sind, sodann die Werte sämtlicher Wurzeln aller dieser Gleichungen durch Auflösung derselben ermitteln und schliesslich die Reihenfolge dieser Wurzeln ebenso wie oben mit Hülfe der Sinustafel oder für $\gamma = 2$ mittelst des in den nachfolgenden Beispielen zu zeigenden Kunstgriffes bestimmen.

Fährt man auf diese Weise fort, so erhält man offenbar schliesslich sämtliche $\frac{n-1}{\zeta}$ Aggregate von ζ Gliedern; entwickelt man daher nach Artikel 348 die Gleichung ζ^{ten} Grades, deren Wurzeln die ζ in $(\zeta, 1)$ enthaltenen Wurzeln aus Ω sind, so sind die Coefficienten dieser sämtlich bekannte Grössen; wenn man nun durch Auflösung nur irgend eine Wurzel findet, so kann man diese gleich $[1]$ setzen, und wird alle übrigen Wurzeln Ω mittelst der Potenzen dieser erhalten. Wenn man lieber will, kann man auch alle Wurzeln jener Gleichung durch Auflösung ermitteln und ausserdem durch Auflösung von $\frac{n-1}{\zeta} - 1$ anderen Gleichungen ζ^{ten} Grades, welche respective alle ζ in den einzelnen noch übrigen Perioden von ζ Gliedern enthaltenen Wurzeln darstellen, alle übrigen Wurzeln Ω finden.

Übrigens ist klar, dass, sobald die erste Gleichung (A) gelöst ist oder sobald man die Werte aller α Aggregate von a Gliedern hat, auch die Zerlegung der Function X in α Factoren von a Dimensionen nach Artikel 348 ohne Weiteres gegeben ist, und ferner dass nach der Auflösung der Gleichung (B) oder nachdem die Werte aller $\alpha\beta$ Aggregate von b Gliedern gefunden sind, jeder einzelne jener Factoren wiederum in β oder X in $\alpha\beta$ Factoren von b Dimensionen zerfällt u. s. w.

353.

Erstes Beispiel für $n = 19$. Da hier $n - 1 = 3 \cdot 3 \cdot 2$ ist, so lässt sich die Ermittlung der Wurzeln Ω auf die Auflösung zweier kubischen und einer quadratischen Gleichung zurückführen. Dies Beispiel wird man um so leichter verstehen, weil die erforderlichen Operationen grösstenteils schon im Vorhergehenden enthalten sind. Nimmt man als primitive Wurzel die Zahl 2, so ergeben sich folgende kleinste Reste ihrer Potenzen (die Exponenten der Potenzen sind in der ersten Reihe den Resten überschrieben):

0.	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
1.	2.	4.	8.	16.	13.	7.	14.	9.	18.	17.	15.	11.	3.	6.	12.	5.	10.

Hieraus leitet man nach den Artikeln 344, 345 leicht die folgende Einteilung sämtlicher Wurzeln Ω in drei Perioden von je sechs, und jeder dieser in drei Perioden von je zwei Gliedern her:

$$\Omega = (18, 1)\begin{cases}(6, 1)\begin{cases}(2,\ 1)\cdots[1], [18]\\(2,\ 8)\cdots[8], [11]\\(2,\ 7)\cdots[7], [12]\end{cases}\\(6, 2)\begin{cases}(2,\ 2)\cdots[2], [17]\\(2, 16)\cdots[3], [16]\\(2, 14)\cdots[5], [14]\end{cases}\\(6, 4)\begin{cases}(2,\ 4)\cdots[4], [15]\\(2, 13)\cdots[6], [13]\\(2,\ 9)\cdots[9], [10].\end{cases}\end{cases}$$

Die Gleichung (A), deren Wurzeln die Aggregate (6, 1), (6, 2), (6, 4) sind, wird

$$x^3 + x^2 - 6x - 7 = 0;$$

eine Wurzel derselben findet man gleich $-1{,}2218761623$. Stellt man diese durch (6, 1) dar, so wird:

$$(6,2) = \quad 4 - \qquad (6,1)^2 = \quad 2{,}5070186441$$
$$(6,4) = -5 - (6,1) + (6,1)^2 = -2{,}2851424818.$$

Hiernach wird X in drei Factoren von 6 Dimensionen zerlegt sein, wenn man diese Werte in Artikel 348 substituiert.

Als Gleichung (B), deren Wurzeln die Aggregate (2, 1), (2, 7), (2, 8) sind, ergiebt sich folgende:

$$x^3 - (6,1)\,x^2 + [(6,1) + (6,4)]\,x - 2 - (6,2) = 0$$

oder:

$$x^3 + 1{,}2218761623x^2 - 3{,}5070186441x - 4{,}5070186441 = 0;$$

eine Wurzel dieser findet man gleich $-1{,}3545631433$, die wir durch (2,1) darstellen. Mittelst der Methode des Artikels 346 aber findet man folgende Gleichungen, in denen der Kürze wegen q für (2, 1) geschrieben ist:

$$(2,2) = q^2 - 2;\ (2,3) = q^3 - 3q;\ (2,4) = q^4 - 4q^2 + 2;\ (2,5) = q^5 - 5q^3 + 5q;$$
$$(2,6) = q^6 - 6q^4 + 9q^2 - 2;\ (2,7) = q^7 - 7q^5 + 14q^3 - 7q;$$
$$(2,8) = q^8 - 8q^6 + 20q^4 - 16q^2 + 2;\ (2,9) = q^9 - 9q^7 + 27q^5 - 30q^3 + 9q.$$

Bequemer als nach den Regeln des Artikels 346 lassen sich diese Gleichungen in diesem Falle durch folgende Betrachtungen entwickeln. Setzt man:

$$[1] = \cos\frac{kP}{19} + i\sin\frac{kP}{19},$$

so wird:

$$[18] = \cos\frac{18kP}{19} + i\sin\frac{18kP}{19} = \cos\frac{kP}{19} - i\sin\frac{kP}{19},\ \text{und somit}\ (2,1) = 2\cos\frac{kP}{19};$$

ebenso allgemein:

$$[\lambda] = \cos\frac{\lambda k P}{19} + i\sin\frac{\lambda k P}{19}, \text{ und daher } (2, \lambda) = [\lambda] + [18\lambda] = \lambda + [-\lambda] = 2\cos\frac{\lambda k P}{19}.$$

Ist daher $\frac{1}{2}q = \cos\omega$, so ist $(2, 2) = 2\cos 2\omega$, $(2, 3) = 2\cos 3\omega$, u. s. w., woraus man nach den bekannten Formeln für die Cosinus vielfacher Winkel dieselben Formeln wie oben ableitet. — Nun erhält man aus diesen Formeln folgende numerische Werte:

$(2, 2) = -0{,}1651586909$	$(2, 6) = 0{,}4909709743$
$(2, 3) = 1{,}5782810188$	$(2, 7) = -1{,}7589475024$
$(2, 4) = -1{,}9727226068$	$(2, 8) = 1{,}8916344834$
$(2, 5) = 1{,}0938963162$	$(2, 9) = -0{,}8033908493.$

Die Werte von (2, 7), (2, 8) können auch aus der Gleichung (B), deren beide andern Wurzeln sie sind, abgeleitet werden, und der Zweifel, welche von diesen Wurzeln (2, 7) und welche (2, 8) ist, lässt sich entweder durch angenäherte Berechnung nach den vorstehend angeführten Formeln oder mit Hülfe der Sinustafeln heben, die bei nur oberflächlicher Benutzung zeigen, dass $(2, 1) = 2\cos\omega$ wird, wenn man $\omega = \frac{7}{19}P$ setzt, wonach

$$(2, 7) = 2\cos\frac{49P}{19} = 2\cos\frac{8P}{19} \quad\text{und}\quad (2, 8) = 2\cos\frac{56P}{19} = 2\cos\frac{P}{19}$$

werden muss. Ebenso kann man die Aggregate (2, 2), (2, 3), (2, 5) auch mittelst der Gleichung

$$x^3 - (6, 2)x^2 + [(6, 1) + (6, 2)]x - 2 - (6, 4) = 0,$$

deren Wurzeln sie sind, finden, und die Ungewissheit, welche Wurzeln jenen Aggregaten bezüglich gleichzusetzen sind, wird in ganz derselben Weise gehoben wie vorher; und ebenso können auch die Aggregate (2, 4), (2, 6), (2, 9) mittelst der Gleichung

$$x^3 - (6, 4)x^2 + [(6, 2) + (6, 4)]x - 2 - (6, 1) = 0$$

gefunden werden.

Endlich sind [1] und [18] die Wurzeln der Gleichung

$$x^2 - (2, 1)x + 1 = 0,$$

und zwar ist die eine von ihnen $= \frac{1}{2}(2, 1) + i\sqrt{1 - \frac{1}{4}(2, 1)^2} = \frac{1}{2}(2, 1) + i\sqrt{\frac{1}{2} - \frac{1}{4}(2, 2)}$, die andere $= \frac{1}{2}(2, 1) - i\sqrt{\frac{1}{2} - \frac{1}{4}(2, 2)}$, und hieraus ihre numerischen Werte: $= -0{,}6772815716 \pm 0{,}7357239107i$. Die sechzehn übrigen Wurzeln können entweder aus der Entwicklung der Potenzen einer jeden dieser beiden Wurzeln oder aus der Auflösung von acht andern ähnlichen Gleichungen abgeleitet werden, wobei in der ersteren Methode entweder mittelst der Sinustafeln oder mit Hülfe des beim folgenden Beispiel zu erklärenden Kunstgriffes entschieden werden muss, für welche der beiden Wurzeln dem imaginären Teile das positive und für welche demselben das negative Vorzeichen vorzusetzen ist. Auf diese Weise wurden die folgenden

Werte gefunden, bei denen das obere Zeichen der ersten, das untere Zeichen der zweiten Wurzel entsprechen soll:

$$\begin{aligned}
[1] \text{ und } [18] &= -0{,}6772815716 \pm 0{,}7357239107\,i \\
[2] \text{ und } [17] &= -0{,}0825793455 \mp 0{,}9965844930\,i \\
[3] \text{ und } [16] &= 0{,}7891405094 \pm 0{,}6142127127\,i \\
[4] \text{ und } [15] &= -0{,}9863613034 \pm 0{,}1645945903\,i \\
[5] \text{ und } [14] &= 0{,}5469481581 \mp 0{,}8371664783\,i \\
[6] \text{ und } [13] &= 0{,}2454854871 \pm 0{,}9694002659\,i \\
[7] \text{ und } [12] &= -0{,}8794737512 \mp 0{,}4759473930\,i \\
[8] \text{ und } [11] &= 0{,}9458172417 \mp 0{,}3246994692\,i \\
[9] \text{ und } [10] &= -0{,}4016954247 \pm 0{,}9157733267\,i
\end{aligned}$$

354.

Zweites Beispiel für $n = 17$. Hier hat man $n - 1 = 2 \cdot 2 \cdot 2 \cdot 2$, so dass die Berechnung der Wurzeln Ω sich auf vier quadratische Gleichungen reducieren lässt. Als primitive Wurzel nehmen wir hier die Zahl 3, deren Potenzen die folgenden kleinsten Reste nach dem Modul 17 liefern:

0.	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.
1.	3.	9.	10.	13.	5.	15.	11.	16.	14.	8.	7.	4.	12.	2.	6.

Hieraus ergeben sich die folgenden Einteilungen des Complexes Ω in zwei Perioden von acht, vier Perioden von vier, acht Perioden von zwei Gliedern:

$$\Omega = (16,1)\begin{cases} (8,1)\begin{cases} (4,\ 1)\begin{cases} (2,\ 1)\cdots[1],[16] \\ (2,13)\cdots[4],[13] \end{cases} \\ (4,\ 9)\begin{cases} (2,\ 9)\cdots[8],[\ 9] \\ (2,15)\cdots[2],[15] \end{cases} \end{cases} \\ (8,3)\begin{cases} (4,\ 3)\begin{cases} (2,\ 3)\cdots[3],[14] \\ (2,\ 5)\cdots[5],[12] \end{cases} \\ (4,10)\begin{cases} (2,10)\cdots[7],[10] \\ (2,11)\cdots[6],[11]. \end{cases} \end{cases} \end{cases}$$

Die Gleichung (A), deren Wurzeln die Aggregate $(8,1)$, $(8,3)$ sind, wird nach den Regeln des Artikel 351: $x^2 + x - 4 = 0$; ihre Wurzeln berechnen sich zu: $-\frac{1}{2} + \frac{1}{2}\sqrt{17} = 1{,}5615528128$ und $-\frac{1}{2} - \frac{1}{2}\sqrt{17} = -2{,}5615528128$; die erstere setzen wir gleich $(8, 1)$, dann ist die andere notwendig gleich $(8, 3)$ zu setzen.

Ferner ergiebt sich als die Gleichung, deren Wurzeln die Aggregate $(4, 1)$ und $(4, 9)$ sind, die folgende (B): $x^2 - (8,1)\,x - 1 = 0$; die Wurzeln dieser sind: $\frac{1}{2}(8,1) \pm \frac{1}{2}\sqrt{4 + (8,1)^2} = \frac{1}{2}(8,1) \pm \frac{1}{2}\sqrt{12 + 3\,(8,1) + 4\,(8,3)}$; diejenige, in welcher der Wurzelgrösse das positive Vorzeichen beigelegt wird, und deren numerischer Wert 2,0494811777 ist, setzen wir gleich $(4, 1)$, wonach die andere, in welcher die Wurzelgrösse negativ genommen wird,

und deren numerischer Wert $-0{,}4879283649$ ist, von selbst durch (4, 9) dargestellt werden muss. Die übrigen Aggregate von vier Gliedern aber, nämlich (4, 3) und (4, 10) können auf doppelte Weise ermittelt werden. Zuerst nämlich nach der Methode des Artikels 346, welche die folgenden Formeln, in denen zur Abkürzung p für (4, 1) geschrieben ist, liefert:

$$(4,3) = -\tfrac{3}{2} + 3p - \tfrac{1}{2}p^3 = 0{,}3441507314$$
$$(4,10) = \tfrac{3}{2} + 2p - p^2 - \tfrac{1}{2}p^3 = -2{,}9057035442.$$

Dieselbe Methode liefert auch die Formel $(4,9) = -1 - 6p + p^2 + p^3$, aus der man denselben Wert findet, den wir vorher angegeben haben. Zweitens aber kann man die Aggregate (4, 3), (4, 10) auch durch Auflösung der Gleichung, deren Wurzeln sie sind, bestimmen. Diese Gleichung wird: $x^2 - (8,3)\,x - 1 = 0$, daher sind ihre Wurzeln $\frac{1}{2}(8,3) \pm \frac{1}{2}\sqrt{4 + (8,3)^2}$ oder $\frac{1}{2}(8,3) + \frac{1}{2}\sqrt{12 + 4(8,1) + 3(8,3)}$ und $\frac{1}{2}(8,3) - \frac{1}{2}\sqrt{12 + 4(8,1) + 3(8,3)}$. Der Zweifel jedoch, welche von diesen beiden Wurzeln man durch (4, 3) und welche man durch (4, 10) ausdrücken muss, lässt sich durch folgenden Kunstgriff, dessen wir im Artikel 352 Erwähnung thaten, heben. Man entwickle das Product aus $(4,1) - (4,9)$ in $(4,3) - (4,10)$, wodurch man $2(8,1) - 2(8,3)$*) erhalten wird; nun ist der Wert dieses Ausdrucks offenbar positiv, nämlich gleich $+2\sqrt{17}$, und überdies ist auch der erste Factor des Products positiv, nämlich $(4,1) - (4,9) = +\sqrt{12 + 3(8,1) + 4(8,3)}$, somit muss notwendig auch der andere Factor $(4,3) - (4,10)$ positiv sein und daher (4, 3) der ersteren Wurzel, in welcher der Wurzelgrösse das positive Vorzeichen vorgesetzt ist, und (4, 10) der letzteren gleichgesetzt werden. Übrigens ergeben sich hieraus dieselben numerischen Werte wie oben.

Nachdem sämtliche Aggregate von vier Gliedern gefunden sind, gehen wir zur Bestimmung der Aggregate von zwei Gliedern. Als Gleichung (C), deren Wurzeln die unter (4, 1) enthaltenen Aggregate (2, 1) und (2, 13) sind, findet man die folgende: $x^2 - (4,1)\,x + (4,3) = 0$; die Wurzeln dieser sind $\frac{1}{2}(4,1) \pm \frac{1}{2}\sqrt{-4(4,3) + (4,1)^2}$ oder $\frac{1}{2}(4,1) \pm \frac{1}{2}\sqrt{4 + (4,9) - 2(4,3)}$. Diejenige, in welcher die Wurzelgrösse positiv genommen und deren Wert gleich 1,8649444588 gefunden wird, setzen wir gleich (2, 1), so dass die andere, deren Wert gleich 0,1845367189 ist, (2, 13) ist. Wenn man die übrigen Aggregate von zwei Gliedern nach der Methode des Artikels 346 ermitteln will, so kann man für (2, 2), (2, 3), (2, 4), (2, 5), (2, 6), (2, 7), (2, 8) dieselben Formeln anwenden, welche wir im vorigen Beispiel für die ebenso bezeichneten Grössen angegeben haben, nämlich (2, 2) [oder (2, 15)] $= (2,1)^2 - 2$, u. s. w. Will man aber lieber je zwei durch Auflösung einer quadratischen

*) Die wahre Natur dieses Ausdrucks besteht darin, dass dieses Product, entwickelt, nicht die Aggregate von vier Gliedern enthält, sondern nur durch Aggregate von acht Gliedern dargestellt werden kann; den Grund hiervon, der der Kürze wegen hier übergangen werden muss, werden Kundige sehr leicht einsehen.

Gleichung berechnen, so findet man für (2, 9) und (2, 15) die Gleichung $x^2 - (4,9)x + (4,10) = 0$, deren Wurzeln sind: $\frac{1}{2}(4,9) \pm \frac{1}{2}\sqrt{4 + (4,1) - 2(4,10)}$; wie man aber hier über das doppelte Vorzeichen verfügen muss, kann ebenso entschieden werden wie oben. Durch Entwicklung des Products aus (2, 1) — (2, 13) und (2, 9) — (2, 15) ergiebt sich nämlich — (4, 1) + (4, 9) — (4, 3) + (4, 10), und da dieses offenbar negativ, der Factor (2, 1) — (2, 13) aber positiv ist, so muss notwendig (2, 9) — (2, 15) negativ sein und daher in dem vorher angegebenen Ausdrucke das obere Zeichen für (2, 15), das untere für (2, 9) genommen werden. Hieraus berechnet man (2, 9) = — 1,9659461994, (2, 15) = 1,4780178344. — Ebenso schliessen wir, da aus der Entwicklung des Products aus (2, 1) — (2, 13) und (2, 3) — (2, 5) sich (4, 9) — (4, 10) und somit eine positive Grösse ergiebt, dass der Factor (2, 3) — (2, 5) positiv ist. Hiernach findet man durch eine ähnliche Rechnung wie vorher:

$$(2, 3) = \tfrac{1}{2}(4, 3) + \tfrac{1}{2}\sqrt{4 + (4, 10) - 2(4, 9)} = 0{,}8914767116$$
$$(2, 5) = \tfrac{1}{2}(4, 3) - \tfrac{1}{2}\sqrt{4 + (4, 10) - 2(4, 9)} = -0{,}5473259801.$$

Endlich findet man durch ganz analoge Operationen:

$$(2, 10) = \tfrac{1}{2}(4, 10) - \tfrac{1}{2}\sqrt{4 + (4, 3) - 2(4, 1)} = -1{,}7004342715$$
$$(2, 11) = \tfrac{1}{2}(4, 10) + \tfrac{1}{2}\sqrt{4 + (4, 3) - 2(4, 1)} = -1{,}2052692728.$$

Wir müssen nun noch zu den Wurzeln Ω selbst herabsteigen. Als Gleichung (*D*), deren Wurzeln [1] und [16] sind, ergiebt sich: $x^2 - (2, 1)x + 1 = 0$, daher die Wurzeln $\frac{1}{2}(2, 1) \pm \frac{1}{2}\sqrt{(2, 1)^2 - 4}$ oder vielmehr $\frac{1}{2}(2, 1) \pm \frac{1}{2}i\sqrt{4 - (2, 1)^2}$ oder $\frac{1}{2}(2, 1) \pm \frac{1}{2}i\sqrt{2 - (2, 15)}$. Das obere Zeichen wählen wir für [1], das untere für [16]. Die vierzehn übrigen Wurzeln erhält man entweder durch Potenzierung von [1] oder durch Auflösung von sieben quadratischen Gleichungen, von denen jede je zwei Wurzeln giebt und wobei die Ungewissheit hinsichtlich der Vorzeichen der Wurzelgrössen durch denselben Kunstgriff beseitigt werden kann, wie im Vorhergehenden. So sind z. B. [4] und [13] die Wurzeln der Gleichung $x^2 - (2, 13)x + 1 = 0$ und daher gleich $\frac{1}{2}(2, 13) \pm \frac{1}{2}i\sqrt{2 - (2, 9)}$. Durch Entwicklung des Products aus [1] — [16] und [4] — [13] aber ergiebt sich (2, 5) — (2, 3) und somit eine reelle negative Grösse; daher muss, weil $[1] - [16] = i\sqrt{2 - (2, 15)}$, d. h. das Product aus der imaginären i in eine positive reelle Grösse ist, auch [4] — [13] wegen $i^2 = -1$ das Product aus i und einer reellen positiven Grösse sein. Hieraus schliesst man, dass für [4] das obere, für [13] das untere Vorzeichen zu nehmen ist. Auf ähnliche Weise findet man für die Wurzeln [8] und [9]: $\frac{1}{2}(2, 9) \pm \frac{1}{2}i\sqrt{2 - (2, 1)}$, wobei, da das Product aus [1] — [16] in [8] — [9] gleich (2, 9) — (2, 10), also negativ wird, für [8] das obere, für [9] das untere Zeichen zu nehmen

ist. Berechnet man ebenso die übrigen Wurzeln, so erhält man die folgenden numerischen Werte, bei denen die oberen Vorzeichen den ersten, die unteren Vorzeichen den letzteren Wurzeln entsprechen:

$$\begin{aligned}
[1],\ [16] &= 0{,}9324722294 \pm 0{,}3612416662\,i\\
[2],\ [15] &= 0{,}7390089172 \pm 0{,}6736956436\,i\\
[3],\ [14] &= 0{,}4457383558 \pm 0{,}8951632914\,i\\
[4],\ [13] &= 0{,}0922683595 \pm 0{,}9957341763\,i\\
[5],\ [12] &= -0{,}2736629901 \pm 0{,}9618256432\,i\\
[6],\ [11] &= -0{,}6026346364 \pm 0{,}7980172273\,i\\
[7],\ [10] &= -0{,}8502171357 \pm 0{,}5264321629\,i\\
[8],\ [\ 9] &= -0{,}9829730997 \pm 0{,}1837495178\,i.
\end{aligned}$$

Das im Vorhergehenden Angegebene könnte zwar zur Auflösung der Gleichung $x^n - 1 = 0$ und daher zur Auffindung der trigonometrischen Functionen, welche mit der Peripherie commensurablen Bogen entsprechen, genügen; indessen können wir wegen der Wichtigkeit des Gegenstandes diese Untersuchung nicht beschliessen, ohne vorher noch aus dem reichen Schatze sowohl von diesen Gegenstand beleuchtenden Bemerkungen als auch von ihm verwandten oder von ihm abhängenden Aufgaben Einiges anzufügen. Hiervon wählen wir insbesondere das aus, was ohne einen grossen Apparat von anderweitigen Untersuchungen erledigt werden kann, und wollen dies nur als Proben dieser sehr umfassenden, später einmal ausführlich zu behandelnden Theorie betrachtet wissen.

Weitere Untersuchungen über die Perioden der Wurzeln. Die Aggregate, in denen die Anzahl der Glieder gerade ist, sind reelle Grössen.

355.

Da n stets als ungerade vorausgesetzt wird, so befindet sich 2 unter den Factoren von $n-1$ und der Complex Ω besteht aus $\frac{1}{2}(n-1)$ Perioden von zwei Gliedern. Eine solche Periode wie $(2, \lambda)$ wird aus $[\lambda]$ und $[\lambda g^{\frac{1}{2}(n-1)}]$ bestehen, wo g wie oben irgend eine primitive Wurzel für den Modul n bedeutet. Es ist aber $g^{\frac{1}{2}(n-1)} \equiv -1$ (mod. n) und daher $\lambda g^{\frac{1}{2}(n-1)} \equiv -\lambda$ (vgl. Artikel 62), somit $[\lambda g^{\frac{1}{2}(n-1)}] = [-\lambda]$. Mithin wird, wenn man $[\lambda] = \cos\frac{kP}{n} + i\sin\frac{kP}{n}$ und somit $[-\lambda] = \cos\frac{kP}{n} - i\sin\frac{kP}{n}$ setzt, das Aggregat $(2, \lambda) = 2\cos\frac{kP}{n}$. Hieraus leiten wir an dieser Stelle nur den Schluss her, dass der Wert eines jeden Aggregats von zwei Gliedern eine reelle Grösse ist. Da jede Periode, deren Gliederanzahl gerade und gleich $2a$ ist, in a Perioden von je zwei Gliedern zerlegt werden kann, so ist der Wert eines jeden Aggregats von gerader Gliederanzahl immer eine reelle

Grösse. Wenn man also im Artikel 352 unter den Factoren $\alpha, \beta, \gamma, \ldots$ die Zahl 2 an die letzte Stelle setzt, so werden sämtliche Operationen, bis man zu Aggregaten von zwei Gliedern kommt, durch reelle Grössen erledigt, und imaginäre werden erst dann eingeführt, wenn man von diesen Aggregaten zu den Wurzeln selbst übergeht.

Über die Gleichung, durch welche die Verteilung der Wurzeln Ω in zwei Perioden bestimmt wird.

356.

Die grösste Beachtung verdienen die Hülfsgleichungen, durch welche für jeden Wert von n die den Complex Ω bildenden Aggregate bestimmt werden, welche in wunderbarer Weise mit den verborgensten Eigenschaften der Zahl n im Zusammenhang stehen. An dieser Stelle aber wollen wir die Untersuchung nur auf die folgenden beiden Fälle beschränken: Zunächst werden wir über die quadratische Gleichung, deren Wurzeln die Aggregate von $\frac{1}{2}(n-1)$ Gliedern sind, sodann für denjenigen Fall, wo $n-1$ den Factor 3 enthält, über die kubische Gleichung, deren Wurzeln die Aggregate von $\frac{1}{3}(n-1)$ Gliedern sind, handeln.

Schreiben wir der Kürze wegen m für $\frac{1}{2}(n-1)$ und bezeichnen wir mit g irgend eine primitive Wurzel für den Modul n, so wird der Complex Ω aus zwei Perioden $(m, 1)$ und (m, g) bestehen, und zwar wird der erstere die Wurzeln $[1], [g^2], [g^4], \ldots, [g^{n-3}]$, der letztere die Wurzeln $[g], [g^3], [g^5], \ldots, [g^{n-2}]$ enthalten. Nimmt man an, dass die kleinsten positiven Reste der Zahlen $g^2, g^4, \ldots, g^{n-3}$ nach dem Modul n, in beliebiger Reihenfolge, $R, R', R'', \ldots$, ebenso die Reste von $g, g^3, \ldots, g^{n-2}$ in beliebiger Reihenfolge $N, N', N'', \ldots$ seien, so werden die Wurzeln, aus denen $(m, 1)$ besteht, mit $[1], [R], [R'], [R''], \ldots$ und die Wurzeln der Periode (m, g) mit $[N], [N'], [N''], \ldots$ übereinstimmen. Nun ist klar, dass sämtliche Zahlen $1, R, R', R'', \ldots$ quadratische Reste der Zahl n sind, und da sie sämtlich verschieden und kleiner als n sind und daher ihre Anzahl gleich $\frac{1}{2}(n-1)$ und somit gleich der Anzahl aller positiven Reste von n unterhalb n ist, so werden diese Reste mit jenen Zahlen ganz und gar übereinstimmen. Hieraus geht von selbst hervor, dass sämtliche Zahlen $N, N', N'', \ldots$, welche sowohl unter sich als auch von $1, R, R', \ldots$ verschieden sind und zusammen mit diesen sämtliche Zahlen $1, 2, 3, \ldots, n-1$ erschöpfen, mit sämtlichen positiven quadratischen Nichtresten von n unterhalb n übereinstimmen müssen. Nimmt man nun an, dass die Gleichung, deren Wurzeln die Aggregate $(m, 1), (m, g)$ sind, die folgende sei:

$$x^2 - Ax + B = 0,$$

so wird:

$$A = (m, 1) + (m, g) = -1, \quad B = (m, 1) \cdot (m, g)$$

Das Product aus $(m, 1)$ und (m, g) ist nach Artikel 345 gleich

$$(m, N+1) + (m, N'+1) + (m, N''+1) + \cdots = W$$

und lässt sich hierauf auf eine Form wie $\alpha(m, 0) + \beta(m, 1) + \gamma(m, g)$ bringen. Zur Bestimmung der Coefficienten α, β, γ bemerken wir erstens, dass $\alpha + \beta + \gamma = m$ ist (da nämlich die Anzahl der Aggregate in W gleich m ist); zweitens, dass $\beta = \gamma$ ist (dies folgt aus Artikel 350, da das Product $(m, 1) \cdot (m, g)$ eine symmetrische Function der Aggregate $(m, 1)$, (m, g) ist, aus denen das grössere Aggregat $(n-1, 1)$ besteht); drittens, da alle Zahlen $N+1$, $N'+1$, $N''+1, \ldots$ innerhalb der Grenzen 2 und $n+1$ excl. enthalten sind, so ist klar, dass entweder kein Aggregat in W auf $(m, 0)$ sich reduciert und daher $\alpha = 0$ ist, wenn unter den Zahlen $N, N', N'', \ldots$ die Zahl $n-1$ nicht vorkommt, oder nur einziges, nämlich (m, n), und somit $\alpha = 1$ wird, wenn $n-1$ sich unter den Zahlen $N, N', N'', \ldots$ vorfindet. Hieraus schliesst man, dass im ersten Falle $\alpha = 0$, $\beta = \gamma = \frac{1}{2}m$; im zweiten $\alpha = 1$, $\beta = \gamma = \frac{1}{2}(m-1)$ ist; gleichzeitig folgt hieraus, da die Zahlen β und γ notwendig ganz sind, dass der erste Fall stattfindet oder $n-1$ (oder, was dasselbe ist, -1) unter den Nichtresten von n nicht enthalten ist, wenn m gerade, also n von der Form $4k+1$ ist; dass aber der zweite Fall stattfindet oder $n-1$ oder -1 unter den Nichtresten von n vorkommt, so oft m ungerade, also n von der Form $4k+3$ ist*). Hiernach wird das gesuchte Product, da $(m, 0) = m$, $(m, 1) + (m, g) = -1$ ist, im ersten Falle gleich $-\frac{1}{2}m$, im zweiten gleich $\frac{1}{2}(m+1)$, und daher die gesuchte Gleichung in jenem Falle: $x^2 + x - \frac{1}{4}(n-1) = 0$, deren Wurzeln $-\frac{1}{2} \pm \frac{1}{2}\sqrt{n}$ sind, in diesem aber: $x^2 + x + \frac{1}{4}(n+1) = 0$, deren Wurzeln $-\frac{1}{2} \pm \frac{1}{2}i\sqrt{n}$ sind.

Welche Wurzel aus Ω also auch für [1] genommen sein möge, die Differenz zwischen den Summen $\Sigma[\mathfrak{R}]$ und $\Sigma[\mathfrak{N}]$, wo für $\mathfrak{R}$ alle positiven quadratischen Reste, für $\mathfrak{N}$ alle Nichtreste von n unterhalb n zu substituieren sind, ist gleich $\pm\sqrt{n}$ für $n \equiv 1$ und gleich $\pm i\sqrt{n}$ für $n \equiv 3 \pmod{4}$. Ebenso folgt hieraus leicht, wenn k irgend eine ganze durch n nicht teilbare Zahl bezeichnet, dass

$$\Sigma \cos\frac{k\mathfrak{R}P}{n} - \Sigma \cos\frac{k\mathfrak{N}P}{n} = \pm\sqrt{n} \quad \text{und} \quad \Sigma \sin\frac{k\mathfrak{R}P}{n} - \Sigma \sin\frac{k\mathfrak{N}P}{n} = 0$$

für $n \equiv 1 \pmod{4}$, dass dagegen für $n \equiv 3 \pmod{4}$ jene Differenz gleich 0 und diese gleich $\pm\sqrt{n}$ ist, Sätze, die wegen ihrer Eleganz höchst bemerkens-

---

*) Auf diese Weise haben wir einen neuen Beweis des Satzes erlangt, dass -1 Rest aller Primzahlen von der Form $4k+1$, Nichtrest aller Primzahlen von der Form $4k+3$ ist, was oben (Artikel 108, 109, 262) bereits auf mehrere verschiedene Arten bewiesen ist. Will man lieber diesen Satz voraussetzen, so ist es nicht nötig, auf die Unterscheidung der beiden verschiedenen Fälle dieser Bedingung Rücksicht zu nehmen, da β, γ schon an sich ganze Zahlen werden.

wert sind. Übrigens bemerken wir, dass die oberen Zeichen stets gelten, wenn für k die Einheit oder allgemeiner ein quadratischer Rest von n, die unteren aber, wenn für k ein quadratischer Nichtrest genommen wird, sowie dass diese Sätze unbeschadet ihrer Eleganz oder vielmehr mit noch grösserer Eleganz auch auf beliebige zusammengesetzte Werte von n ausgedehnt werden können; über dieses aber, welches einer tieferen Untersuchung bedarf, können wir an dieser Stelle nicht reden, müssen uns vielmehr die Betrachtung desselben für eine andere Gelegenheit vorbehalten.

Beweis eines im vierten Abschnitt erwähnten Satzes.

357.

Ist die Gleichung m^{ten} Grades, deren Wurzeln die m in der Periode $(m, 1)$ enthaltenen Wurzeln sind, die folgende:

$$x^m - ax^{m-1} + bx^{m-2} - \cdots = 0$$

oder $z = 0$, so ist $a = (m, 1)$ und die übrigen Coefficienten $b, \ldots$ sind unter einer solchen Form $\mathfrak{A} + \mathfrak{B}(m, 1) + \mathfrak{C}(m, g)$ enthalten, so dass $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ ganze Zahlen sind (Artikel 348), und bezeichnet man mit z' die Function, in welche z übergeht, wenn für $(m, 1)$ überall (m, g) und für (m, g) überall (m, g^2) oder, was dasselbe ist, $(m, 1)$ substituiert wird, so sind die Wurzeln der Gleichung $z' = 0$ die in (m, g) enthaltenen Wurzeln, und das Product

$$zz' = \frac{x^n - 1}{x - 1} = X.$$

Es kann daher z auf eine Form wie $R + S(m, 1) + T(m, g)$ gebracht werden, wo R, S, T ganze Functionen von x sind, deren sämtliche Coefficienten ebenfalls ganze Zahlen sind. Ist dies geschehen, so hat man:

$$z' = R + S(m, g) + T(m, 1).$$

Hieraus folgt, wenn man der Kürze wegen p und q für $(m, 1)$ und (m, g) respective schreibt:

$$2z = 2R + (S+T)(p+q) - (T-S)(p-q) = 2R - S - T - (T-S)(p-q)$$

und analog:

$$2z' = 2R - S - T + (T-S)(p-q).$$

Setzt man daher:

$$2R - S - T = Y, \quad T - S = Z,$$

so folgt hieraus: $4X = Y^2 - (p-q)^2 Z^2$, und daher, weil $(p-q)^2 = \pm n$ ist:

$$4X^2 = Y^2 \mp nZ^2,$$

wobei das obere Zeichen gilt, wenn n von der Form $4k+1$, das untere, wenn n von der Form $4k+3$ ist. Dies ist der Satz, dessen Beweis wir

oben (Artikel 124) versprochen haben. Man sieht leicht, dass die beiden höchsten Glieder von Y stets $2x^m + x^{m-1}$ sind und das höchste Glied der Function Z stets x^{m-1} wird; die übrigen Coefficienten aber, die offenbar sämtlich ganze Zahlen sind, sind verschieden für verschiedene Beschaffenheit der Zahl n und lassen sich nicht unter eine allgemeine analytische Formel bringen.

Beispiel. Für $n = 17$ findet man als diejenige Gleichung, deren Wurzeln die acht in (8, 1) enthaltenen Wurzeln sind, nach den Regeln im Artikel 348:

$$x^8 - px^7 + (4 + p + 2q)x^6 - (4p + 3q)x^5 + (6 + 3p + 5q)x^4 - (4p + 3q)x^3 + (4 + p + 2q)x^2 - px + 1 = 0,$$

woraus sich ergiebt:

$$R = x^8 + 4x^6 + 6x^4 + 4x^2 + 1$$
$$S = -x^7 + x^6 - 4x^5 + 3x^4 - 4x^3 + x^2 - x$$
$$T = 2x^6 - 3x^5 + 5x^4 - 3x^3 + 2x^2$$

und hieraus

$$Y = 2x^8 + x^7 + 5x^6 + 7x^5 + 4x^4 + 7x^3 + 5x^2 + x + 2$$
$$Z = x^7 + x^6 + x^5 + 2x^4 + x^3 + x^2 + 2.$$

Hier sind noch einige andere Beispiele:

n	Y	Z
3	$2x + 1$	1
5	$2x^2 + x + 2$	x
7	$2x^3 + x^2 - x - 2$	$x^2 + x$
11	$2x^5 + x^4 - 2x^3 + 2x^2 - x - 2$	$x^4 + x$
13	$2x^6 + x^5 + 4x^4 - x^3 + 4x^2 + x + 2$	$x^5 + x^3 + x$
19	$2x^9 + x^8 - 4x^7 + 3x^6 + 5x^5 - 5x^4 - 3x^3 + 4x^2 - x - 2$	$x^8 - x^6 + x^5 + x^4 - x^3 + x$
23	$2x^{11} + x^{10} - 5x^9 - 8x^8 - 7x^7 - 4x^6 + 4x^5 + 7x^4 + 8x^3 + 5x^2 - x - 2$	$x^{10} + x^9 - x^7 - 2x^6 - 2x^5 - x^4 + x^2 + x.$

Über die Gleichung für die Verteilung der Wurzeln Ω in drei Perioden.

358.

Wir gehen zur Betrachtung der kubischen Gleichungen über, durch welche in dem Falle, wo n von der Form $3k + 1$ ist, die drei Aggregate von $\frac{1}{3}(n - 1)$ Gliedern, welche den Complex Ω bilden, bestimmt werden. Es sei g irgend eine primitive Wurzel für den Modul n und $\frac{1}{3}(n - 1) = m$, welches eine gerade ganze Zahl ist. Dann sind die drei Aggregate, aus denen Ω besteht, $(m, 1)$, (m, g), (m, g^2), für welche wir p, p', p'' schreiben

werden, und es ist klar, dass das erste die Wurzeln $[1]$, $[g^3]$, $[g^6]$, ..., $[g^{n-4}]$, das zweite die Wurzeln $[g]$, $[g^4]$, ..., $[g^{n-3}]$, das dritte die Wurzeln $[g^2]$, $[g^5]$, ..., $[g^{n-2}]$ enthält. Nimmt man an, dass die gesuchte Gleichung

$$x^3 - Ax^2 + Bx - C = 0$$

sei, so wird:

$$A = p + p' + p'', \quad B = pp' + p'p'' + pp'', \quad C = pp'p'',$$

woraus man sogleich $A = -1$ erhält. Es seien die kleinsten positiven Reste der Zahlen g^3, g^6, ..., g^{n-4} nach dem Modul n in willkürlicher Reihenfolge: $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, ... und $\mathfrak{K}$ der Complex derselben, wenn man noch die Zahl 1 hinzufügt; ebenso seien $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$, ... die kleinsten positiven Reste der Zahlen g, g^4, g^7, ..., g^{n-3} und $\mathfrak{K}'$ ihr Complex; endlich seien $\mathfrak{A}''$, $\mathfrak{B}''$, $\mathfrak{C}''$, ... die kleinsten positiven Reste von g^2, g^5, g^8, ..., g^{n-2} und $\mathfrak{K}''$ ihr Complex; dann werden also die Zahlen in $\mathfrak{K}$, $\mathfrak{K}'$, $\mathfrak{K}''$ sämtlich von einander verschieden und mit den folgenden $1, 2, 3, \ldots, n-1$ identisch sein. Vor allem muss hier bemerkt werden, dass die Zahl $n-1$ notwendig in $\mathfrak{K}$ sich vorfindet, da man leicht sieht, dass dieselbe Rest von $g^{\frac{3m}{2}}$ ist. Hieraus folgt auch leicht, dass zwei Zahlen wie h und $n-h$ in ebendemselben Complex von den dreien $\mathfrak{K}$, $\mathfrak{K}'$, $\mathfrak{K}''$ vorkommen müssen, denn wenn die eine Rest von g^λ ist, ist die andere Rest von $g^{\lambda + \frac{3m}{2}}$ oder von $g^{\lambda - \frac{3m}{2}}$, wenn $\lambda > \frac{3m}{2}$ ist. Wir bezeichnen mit $(\mathfrak{K}\mathfrak{K})$ die Anzahl der Zahlen in der Reihe $1, 2, 3, \ldots, n-1$ von solcher Art, dass sie nicht nur selbst, sondern auch die um eine Einheit grösseren Zahlen in $\mathfrak{K}$ enthalten sind, ebenso mit $(\mathfrak{K}\mathfrak{K}')$ die Anzahl der Zahlen in derselben Reihe, welche in $\mathfrak{K}$ enthalten sind, während die auf sie unmittelbar folgenden Zahlen in $\mathfrak{K}'$ enthalten sind, woraus zugleich die Bedeutung der Bezeichnungen $(\mathfrak{K}\mathfrak{K}'')$, $(\mathfrak{K}'\mathfrak{K})$, $(\mathfrak{K}'\mathfrak{K}')$, $(\mathfrak{K}'\mathfrak{K}'')$, $(\mathfrak{K}''\mathfrak{K})$, $(\mathfrak{K}''\mathfrak{K}')$, $(\mathfrak{K}''\mathfrak{K}'')$ von selbst klar ist. Sodann behaupten wir erstens, dass $(\mathfrak{K}\mathfrak{K}') = (\mathfrak{K}'\mathfrak{K})$ ist. Denn nehmen wir an, dass h, h', h'', ... sämtliche Zahlen der Reihe $1, 2, 3, \ldots, n-1$ seien, welche selbst in $\mathfrak{K}$ enthalten sind, während die nächstgrösseren Zahlen $h+1$, $h'+1$, $h''+1$, ... in $\mathfrak{K}'$ enthalten sind, und deren Anzahl somit gleich $(\mathfrak{K}\mathfrak{K}')$ ist, so ist klar, dass alle Zahlen $n-h-1$, $n-h'-1$, $n-h''-1$, ... in $\mathfrak{K}'$, die nächstgrösseren $n-h$, $n-h'$, ... aber in $\mathfrak{K}$ enthalten sind; mithin kann, da es solcher Zahlen überhaupt $(\mathfrak{K}'\mathfrak{K})$ giebt, sicher nicht $(\mathfrak{K}'\mathfrak{K}) < (\mathfrak{K}\mathfrak{K}')$ sein, und ebenso wird bewiesen, dass nicht $(\mathfrak{K}\mathfrak{K}') < (\mathfrak{K}'\mathfrak{K})$ sein kann; daher müssen beide Zahlen notwendig gleich sein. Auf ganz dieselbe Weise beweist man, dass $(\mathfrak{K}\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K})$, $(\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}')$ ist. Zweitens ist, da notwendig jeder Zahl in $\mathfrak{K}$, die grösste $n-1$ allein ausgenommen, eine nächstgrössere Zahl folgen muss, die entweder in $\mathfrak{K}$ oder in $\mathfrak{K}'$ oder in $\mathfrak{K}''$ enthalten ist, die Summe $(\mathfrak{K}\mathfrak{K}) + (\mathfrak{K}\mathfrak{K}') + (\mathfrak{K}\mathfrak{K}'')$ gleich

der um eine Einheit verminderten Anzahl aller Zahlen, nämlich gleich $m-1$, und aus ähnlichem Grunde ist:

$$(\mathfrak{K}'\mathfrak{K}) + (\mathfrak{K}'\mathfrak{K}') + (\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}) + (\mathfrak{K}''\mathfrak{K}') + (\mathfrak{K}''\mathfrak{K}'') = m.$$

Nach diesen Vorbereitungen entwickeln wir nach den Vorschriften des Artikels 345 das Product pp' in $(m, \mathfrak{A}'+1) + (m, \mathfrak{B}'+1) + (m, \mathfrak{C}'+1) + \cdots$, welcher Ausdruck sich, wie man leicht sieht, auf $(\mathfrak{K}'\mathfrak{K})p + (\mathfrak{K}'\mathfrak{K}')p' + (\mathfrak{K}'\mathfrak{K}'')p''$ reduciert, und da nach Artikel 345 I das Product $p'p''$ aus jenem entsteht, wenn man für $(m, 1)$, (m, g), (m, g^2) respective (m, g), (m, g^2), (m, g^3) d. h. für p, p', p'' respective p', p'', p setzt, so wird $p'p'' = (\mathfrak{K}'\mathfrak{K})p' + (\mathfrak{K}'\mathfrak{K}')p'' + (\mathfrak{K}'\mathfrak{K}'')p$ und auf ganz ähnliche Weise $p''p = (\mathfrak{K}'\mathfrak{K})p'' + (\mathfrak{K}'\mathfrak{K}')p + (\mathfrak{K}'\mathfrak{K}'')p'$. Hieraus folgt sofort: Erstens:

$$B = m(p + p' + p'') = -m;$$

zweitens: Da sich in ähnlicher Weise, wie vorher pp' entwickelt wurde, auch pp'' auf $(\mathfrak{K}''\mathfrak{K})p + (\mathfrak{K}''\mathfrak{K}')p' + (\mathfrak{K}''\mathfrak{K}'')p''$ reduciert und dieser Ausdruck mit dem vorigen identisch sein muss, so ist notwendig: $(\mathfrak{K}''\mathfrak{K}) = (\mathfrak{K}'\mathfrak{K}')$ und $(\mathfrak{K}''\mathfrak{K}'') = (\mathfrak{K}'\mathfrak{K})$. Hieraus folgt, wenn man

$$(\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}') = a, \quad (\mathfrak{K}''\mathfrak{K}'') = (\mathfrak{K}'\mathfrak{K}) = (\mathfrak{K}\mathfrak{K}') = b,$$
$$(\mathfrak{K}'\mathfrak{K}') = (\mathfrak{K}''\mathfrak{K}) = (\mathfrak{K}\mathfrak{K}'') = c$$

setzt, dass $m - 1 = (\mathfrak{K}\mathfrak{K}) + (\mathfrak{K}\mathfrak{K}') + (\mathfrak{K}\mathfrak{K}'') = (\mathfrak{K}\mathfrak{K}) + b + c$ und $a + b + c = m$, also $(\mathfrak{K}\mathfrak{K}) = a - 1$ ist, so dass jene neun unbekannten Grössen auf drei, a, b, c, oder vielmehr wegen der Gleichung $a + b + c = m$ auf zwei reduciert sind. Endlich wird das Quadrat p offenbar in $(m, 1 + 1) + (m, \mathfrak{A} + 1) + (m, \mathfrak{B} + 1) + (m, \mathfrak{C} + 1) + \cdots$ entwickelt; unter den Teilen dieses Ausdrucks findet sich (m, n), welches sich auf $(m, 0)$ oder m reduciert, während sich die übrigen, wie man leicht sieht, auf $(\mathfrak{K}\mathfrak{K})p + (\mathfrak{K}\mathfrak{K}')p' + (\mathfrak{K}\mathfrak{K}'')p''$ reducieren; daher hat man: $p^2 = m + (a-1)p + bp' + cp''$.

Auf diese Weise haben wir also durch vorstehende Untersuchungen die folgenden vier Reductionen erhalten:

$$\begin{aligned} p^2 &= m + (a-1)p + bp' + cp'' \\ pp' &= bp + cp' + ap'' \\ pp'' &= cp + ap' + bp'' \\ p'p'' &= ap + bp' + cp'', \end{aligned}$$

wo zwischen den drei unbekannten Grössen a, b, c die Bedingungsgleichung

$$\text{(I)} \qquad a + b + c = m$$

stattfindet und überdies sicher ist, dass sie ganze Zahlen sind. Hieraus folgt:

$$\begin{aligned} C = p \cdot p'p'' &= ap^2 + bpp' + cpp'' \\ &= am + (a^2 + b^2 + c^2 - a)p + (ab + bc + ac)p' + (ab + bc + ac)p''. \end{aligned}$$

Da aber $pp'p''$ eine symmetrische Funktion der drei Aggregate p, p', p'' ist, so sind die Coefficienten, mit denen diese in dem vorstehenden Aus-

drucke multipliciert sind, notwendig einander gleich, wodurch man die neue Gleichung erhält:

$$\text{(II)} \qquad a^2 + b^2 + c^2 - a = ab + bc + ac$$

und hieraus $C = am + (ab + bc + ca)(p + p' + p'')$ oder (wegen (I) und $p + p' + p'' = -1$):

$$\text{(III)} \qquad C = a^2 - bc$$

Obwohl nun C hier von den drei Unbekannten, zwischen denen man nur zwei Gleichungen hat, abhängt, so genügen doch diese mit Zuhülfenahme der Bedingung, dass a, b, c ganze Zahlen sind, zur vollständigen Bestimmung von C. Um dies zu zeigen, stellen wir die Gleichung (II) in der Form dar:

$$12a + 12b + 12c + 4 = 36a^2 + 36b^2 + 36c^2 - 36ab - 36ac - 36bc - 24a + 12b + 12c + 4.$$

Die linke Seite wird nach (I) gleich $12m + 4 = 4n$, die rechte aber reduciert sich auf:

$$(6a - 3b - 3c - 2)^2 + 27(b - c)^2,$$

oder, wenn man k für $2a - b - c$ schreibt, auf $(3k - 2)^2 + 27(b - c)^2$. Hieraus geht hervor, dass die Zahl $4n$ (d. h. allgemein das Vierfache jeder Primzahl von der Form $3m + 1$) durch die Form $x^2 + 27y^2$ dargestellt werden kann, ein Resultat, welches allerdings leicht aus der Theorie der binären Formen abgeleitet werden kann; immerhin ist es merkwürdig genug, dass eine solche Zerlegung mit den Werten von a, b, c zusammenhängt. Die Zahl $4n$ lässt sich aber immer nur auf eine einzige Weise in ein Quadrat und das Siebenundzwanzigfache eines Quadrats zerlegen, was wir auf folgende Art beweisen.*) Nähme man

$$4n = t^2 + 27u^2 = t'^2 + 27u'^2$$

an, so würde sein: Erstens:

$$(tt' - 27uu')^2 + 27(tu' + t'u)^2 = 16n^2;$$

zweitens:

$$(tt' + 27uu')^2 + 27(tu' - t'u)^2 = 16n^2,$$

drittens:

$$(tu' + t'u)(tu' - t'u) = 4n(u'^2 - u^2).$$

Aus der dritten Gleichung folgt, dass n, da es eine Primzahl ist, in einer der beiden Zahlen $tu' + t'u$, $tu' - t'u$ aufgeht; aus der ersten und zweiten

*) Directer liesse sich dieser Satz nach den Prinzipien des fünften Abschnitts beweisen.

aber geht hervor, dass jede dieser Zahlen kleiner als n ist; daher muss diejenige, welche durch n teilbar ist, notwendig gleich 0 sein, und daher auch $u'^2 - u^2 = 0$, daher $u'^2 = u^2$ und $t'^2 = t^2$, d. h. jene beiden Zerlegungen sind nicht verschieden. Wenn wir daher die Zerlegung von $4n$ in ein Quadrat und das Siebenundzwanzigfache eines Quadrats als bekannt voraussetzen (eine Zerlegung, die man entweder nach der im fünften Abschnitt angegebenen directen oder nach der in den Artikeln 323, 324 dargelegten indirecten Methode ermitteln kann), wenn wir nämlich haben: $4n = M^2 + 27N^2$, so sind die Quadrate $(3k-2)^2$, $(b-c)^2$ bestimmt, und an Stelle der Gleichung (II) haben wir nunmehr zwei erlangt. Man sieht aber leicht, dass nicht nur das Quadrat $(3k-2)^2$, sondern auch seine Wurzel $3k-2$ vollständig bestimmt ist; denn da sie notwendig entweder gleich $+M$ oder gleich $-M$ sein muss, so wird die Zweideutigkeit im Vorzeichen durch die Bedingung, dass k eine ganze Zahl sein soll, aufgehoben werden. Man hat nämlich $3k-2 = +M$ oder $= -M$ zu setzen, je nachdem M von der Form $3z+1$ oder $3z+2$ ist*). Da nun $k = 2a - b - c = 3a - m$ ist, so wird $a = \frac{1}{3}(m+k)$, $b + c = m - a = \frac{1}{3}(2m - k)$, und daher:

$$C = a^2 - bc = a^2 - \tfrac{1}{4}(b+c)^2 + \tfrac{1}{4}(b-c)^2$$
$$= \tfrac{1}{9}(m+k)^2 - \tfrac{1}{36}(2m-k)^2 + \tfrac{1}{4}N^2 = \tfrac{1}{12}k^2 + \tfrac{1}{3}km + \tfrac{1}{4}N^2,$$

und auf diese Weise sind sämtliche Coefficienten gefunden. — Diese Formel wird noch einfacher, wenn für N^2 sein Wert aus der Gleichung $(3k-2)^2 + 27N^2 = 4n = 12m + 4$ substituiert wird, wodurch man nach ausgeführter Rechnung erhält:

$$C = \tfrac{1}{9}(m + k + 3km) = \tfrac{1}{9}(m + kn).$$

Derselbe Wert lässt sich auch auf $(3k-2)N^2 + k^3 - 2k^2 + k - km + m$ reducieren, ein Ausdruck, der zwar für die Anwendung weniger geeignet ist, aber doch sogleich zeigt, dass C, wie es sein soll, sicher eine ganze Zahl wird.

Beispiel. Für $n = 19$ wird $4n = 49 + 27$, daher $3k - 2 = +7$, $k = 3$, $C = \frac{1}{9}(6 + 57) = 7$ und die gesuchte Gleichung ist $x^3 + x^2 - 6x - 7 = 0$, wie oben (Artikel 351). — Auf ähnliche Weise ergiebt sich für $n = 7$, 13, 31, 37, 43, 61, 67 der Wert von k respective gleich 1, -1, 2, -3, -2, 1, -1, daher $C = 1$, -1, 8, -11, -8, 9, -5.

Obwohl übrigens das in diesem Artikel gelöste Problem ziemlich verwickelt ist, so haben wir es doch nicht unterdrücken wollen, einmal wegen

---

*) Offenbar kann nicht M von der Form $3z$ sein, denn sonst würde $4n$ durch 3 teilbar werden. — Auf die Zweideutigkeit, ob $b - c = N$ oder $= -N$ zu setzen sei, braucht man hier weiter keine Rücksicht zu nehmen, und lässt sich dieselbe auch der Natur der Sache nach nicht beseitigen, da dies von der Wahl der primitiven Wurzel g abhängt, so dass für einige primitive Wurzeln die Differenz $b - c$ positiv, für andere negativ wird.

der Eleganz der Lösung, sodann weil es Gelegenheit gab, verschiedene Kunstgriffe zu benutzen, welche auch bei andern Untersuchungen mit hervorragendem Nutzen angewendet werden können.*)

Zurückführung der Gleichungen, durch welche die Wurzeln Ω gefunden werden, auf reine Gleichungen.

359.

Die vorstehenden Untersuchungen handeln von der Auffindung der Hülfsgleichungen; jetzt wollen wir hinsichtlich ihrer Auflösung eine sehr hervorragende Eigenschaft derselben darlegen. Bekanntlich sind alle Bemühungen der grössten Geometer, die allgemeine Auflösung der Gleichungen, welche den vierten Grad übersteigen, oder (um genauer zu definieren, was man will) die **Reduction der gemischten Gleichungen auf reine** Gleichungen zu finden, bisher stets vergeblich gewesen, und es bleibt kaum zweifelhaft, dass dieses Problem nicht sowohl die Kräfte der heutigen Analysis übersteigt, als vielmehr etwas Unmögliches erreichen will. (Man vergleiche, was wir hierüber in der Abhandlung: *Demonstratio nova* etc. Artikel 9 angemerkt haben.) Nichtsdestoweniger ist es sicher, dass es unzählig viele gemischte Gleichungen jeden Grades giebt, welche eine solche Zurückführung auf reine Gleichungen gestatten, und wir hoffen, dass es den Geometern nicht unerwünscht sein wird, wenn wir zeigen, dass unsere Hülfsgleichungen immer hierher gehören. Wegen des grossen Umfanges dieser Untersuchung aber geben wir an dieser Stelle nur die Hauptmomente an, welche zum Beweise der Möglichkeit erforderlich sind, und verschieben eine ausführlichere Behandlung, deren dieser Gegenstand äusserst wert ist, auf eine andere Zeit. Vorausgeschickt müssen einige allgemeine Bemerkungen über die Wurzeln der Gleichung $x^e - 1 = 0$ werden, welche auch denjenigen Fall umfassen, wo e eine zusammengesetzte Zahl ist.

I. Diese Wurzeln werden (wie aus den Elementarbüchern bekannt ist) durch $\cos\frac{kP}{e} + i\,\sin\frac{kP}{e}$ dargestellt, wo für k die e Zahlen $0, 1, 2, 3, \ldots, e-1$ oder irgendwelche andern diesen nach dem Modul e congruente Zahlen zu nehmen sind. Eine Wurzel, für $k = 0$ oder allgemein für einen durch e teilbaren Wert von k, wird gleich 1; jedem andern Werte von k entspricht eine von 1 verschiedene Wurzel.

---

*) Folgerung. Ist ε eine Wurzel der Gleichung $x^3 - 1 = 0$, so hat man: $(p + \varepsilon p' + \varepsilon^2 p'')^3 = \frac{n}{2}(M + N\sqrt{-27})$. Setzt man $\frac{M}{\sqrt{4n}} = \cos\varphi, \frac{N\sqrt{27}}{\sqrt{4n}} = \sin\varphi$, so ist: $p = -\frac{1}{3} + \frac{2}{3}\cos\frac{1}{3}\varphi\sqrt{n}$, $M \equiv +1 \pmod{3}$; $1 \equiv M(1\cdot 2\cdot 3\cdots m)^3 \pmod{n}$. Setzt man $3x + 1 = y$, so wird die Gleichung: $y^3 - 3ny - Mn = 0$.

II. Da $\left(\cos\frac{kP}{e}+i\,\sin\frac{kP}{e}\right)^{\lambda}=\cos\frac{\lambda kP}{e}+i\,\sin\frac{\lambda kP}{e}$ ist, so ist klar, dass, wenn R eine Wurzel ist, welche einem zu e primen Werte von k entspricht, in der Progression R, R^2, R^3, ... das e^{te} Glied allerdings gleich 1 ist, alle vorhergehenden aber von 1 verschieden sind. Hieraus folgt sogleich, dass alle e Grössen $1, R, R^2, R^3, \ldots, R^{e-1}$ ungleich sind und, da offenbar alle der Gleichung $x^e - 1 = 0$ genügen, sämtliche Wurzeln dieser Gleichung darstellen.

III. Endlich wird unter derselben Voraussetzung das Aggregat

$$1+R^{\lambda}+R^{2\lambda}+\cdots+R^{\lambda(e-1)}=0$$

für jeden ganzen, durch e nicht teilbaren Wert von λ; denn dasselbe ist gleich $\frac{1-R^{\lambda e}}{1-R^{\lambda}}$, und der Zähler dieses Bruches wird gleich 0, der Nenner aber nicht gleich 0. Ist aber λ durch e teilbar, so ist jenes Aggregat offenbar gleich e.

360.

Es sei, wie immer im Vorhergehenden, n eine Primzahl, g eine primitive Wurzel für den Modul n und $n-1$ das Product aus drei ganzen positiven Zahlen α, β, γ. Der Kürze wegen werden wir die Untersuchung sogleich so anstellen, dass sie sich auch auf die Fälle, wo α oder γ gleich 1 ist, erstreckt; wenn $\gamma=1$ ist, so muss man für die Aggregate $(\gamma, 1)$, (γ, g), ... die Wurzeln $[1]$, $[g]$, ... nehmen. Wir nehmen also an, dass aus allen, als bekannt vorausgesetzten α Aggregaten von $\beta\gamma$ Gliedern $(\beta\gamma, 1)$ $(\beta\gamma, g)$, $(\beta\gamma, g^2), \ldots, (\beta\gamma, g^{\alpha-1})$ die Aggregate von γ Gliedern abgeleitet werden sollen, eine Aufgabe, die wir oben auf eine gemischte Gleichung β^{ten} Grades reduciert haben, von der wir aber zeigen werden, wie man sie durch eine reine ebenso hohe Gleichung erledigen kann. Zur Abkürzung werden wir für die Aggregate

$$(\gamma, 1), (\gamma, g^{\alpha}), (\gamma, g^{2\alpha}), \ldots, (\gamma, g^{\alpha\beta-\alpha}),$$

welche unter $(\beta\gamma, 1)$ enthalten sind, bezüglich $a, b, c, \ldots, m$, für die folgenden:

$$(\gamma, g), (\gamma, g^{\alpha+1}), (\gamma, g^{2\alpha+1}), \ldots, (\gamma, g^{\alpha\beta-\alpha+1}),$$

welche unter $(\beta\gamma, g)$ enthalten sind, bezüglich $a', b', c', \ldots, m'$, für

$$(\gamma, g^2), (\gamma, g^{\alpha+2}), \ldots., (\gamma, g^{\alpha\beta-\alpha+2})$$

bezüglich $a'', b'', \ldots, m''$ schreiben, u. s. w. bis zu denjenigen, welche in $(\beta\gamma, g^{\alpha-1})$ enthalten sind.

I. Es bezeichne nun R unbestimmt irgend eine Wurzel der Gleichung $x^\beta - 1 = 0$, und es werde angenommen, dass aus der Entwickelung der β^{ten} Potenz der Function

$$t = a + Rb + R^2c + \cdots + R^{\beta-1}m$$

nach den Regeln des Artikels 345 sich ergebe:

$$\begin{aligned} N + Aa &+ Bb + Cc + \cdots + Mm \\ &+ A'a' + B'b' + C'c' + \cdots + M'm' \\ &+ A''a'' + B''b'' + C''c'' + \cdots + M''m'' \\ &+ \cdots\cdots\cdots\cdots\cdots\cdots = T, \end{aligned}$$

wo sämtliche Coefficienten $N, A, B, A', \ldots$ rationale ganze Functionen von R sein werden. Nimmt man ferner an, dass die β^{ten} Potenzen zweier andern Functionen

$$u = R^\beta a + Rb + R^2c + \cdots + R^{\beta-1}m,$$
$$u' = b + Rc + R^2d + \cdots + R^{\beta-2}m + R^{\beta-1}a$$

respective in U und U' entwickelt werden, so erkennt man aus Artikel 350 leicht, da u' aus t entsteht, wenn man die Aggregate $a, b, c, \ldots, m$ bezüglich mit $b, c, d, \ldots, a$ vertauscht, dass

$$\begin{aligned} U' = N + Ab &+ Bc + Cd + \cdots + Ma \\ &+ A'b' + B'c' + C'd' + \cdots + M'a' \\ &+ A''b'' + B''c'' + C''d'' + \cdots + M''a'' \\ &+ \cdots\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

ist. Ferner wird offenbar, da $u = Ru'$ ist, $U = R^\beta U'$; mithin sind wegen $R^\beta = 1$ die entsprechenden Coefficienten in U und U' gleich; schliesslich erkennt man leicht, dass, weil sich t und u nur dadurch unterscheiden, dass a in t mit der Einheit, in u aber mit R^β multipliciert ist, alle entsprechenden Coefficienten (d. h. diejenigen, mit denen dieselben Aggregate multipliciert sind) in T und U und somit auch alle entsprechenden Coefficienten in T und U' gleich sind. Hieraus folgt endlich $A = B = C = \cdots = M$, $A' = B' = C' = \cdots = M'$, $A'' = B'' = C'' = \cdots = M''$, $\cdots$, so dass hierdurch T reduciert wird auf eine solche Form:

$$N + A(\beta\gamma, 1) + A'(\beta\gamma, g) + A''(\beta\gamma, g^2) + \cdots,$$

wo man die einzelnen Coefficienten $N, A, A', \ldots$ auf eine solche Form

$$pR^{\beta-1} + p'R^{\beta-2} + p''R^{\beta-3} + \cdots$$

bringen kann, dass $p, p', p'', \ldots$ gegebene ganze Zahlen sind.

II. Nimmt man für R eine bestimmte Wurzel der Gleichung $x^\beta - 1 = 0$ (von der wir voraussetzen, dass wir ihre Lösung schon haben) und zwar eine solche, dass keine niedrigere Potenz von ihr als die β^{te} der Einheit gleich ist, so ist auch T eine bestimmte Grösse, aus der man t vermit-

telst der reinen Gleichung $t^\beta - T = 0$ ableiten kann. Da aber diese Gleichung β Wurzeln hat, welche $t, Rt, R^2t, \ldots, R^{\beta-1}t$ sind, so kann es zweifelhaft erscheinen, welche Wurzel man nehmen muss. Dass dies aber völlig willkürlich ist, wird leicht in folgender Weise klar werden. Man muss sich erinnern, dass, nachdem sämtliche Aggregate von $\beta\gamma$ Gliedern bestimmt sind, die Wurzel [1] nur insoweit bestimmt ist, dass irgend eine von den $\beta\gamma$ in $(\beta\gamma, 1)$ enthaltenen Wurzeln mit diesem Zeichen bezeichnet sein muss, und es somit völlig willkürlich ist, welches von den β das Aggregat $(\beta\gamma, 1)$ bildenden Aggregaten wir mit a bezeichnen wollen. Wenn man nun, nachdem irgend ein bestimmtes Aggregat durch a dargestellt ist, annimmt, dass $t = \mathfrak{T}$ werde, so sieht man leicht, dass, wenn man nachher dasselbe Aggregat, welches eben mit b bezeichnet wurde, mit a bezeichnen wollte, diejenigen Aggregate, welche vorher $c, d, \ldots, a, b$ waren, jetzt $b, c, \ldots m, a$ sein würden und daher der Wert von t jetzt gleich $\frac{\mathfrak{T}}{R} = \mathfrak{T}R^{\beta-1}$ werden würde. Ebenso würde, wenn man mit a dasjenige Aggregat bezeichnen wollte, welches anfänglich c war, der Wert von t gleich $\mathfrak{T}R^{\beta-2}$ werden, und so kann ferner t irgend einer der Grössen $\mathfrak{T}, \mathfrak{T}R^{\beta-1}, \mathfrak{T}R^{\beta-2}, \ldots$ d. h. irgend einer der Wurzeln der Gleichung $x^\beta - T = 0$ als gleich betrachtet werden, je nachdem man annimmt, dass dies oder jenes in $(\beta\gamma, 1)$ enthaltene Aggregat mit $(\gamma, 1)$ bezeichnet werde.

III. Nachdem die Grösse t auf diese Weise bestimmt ist, muss man $\beta - 1$ andere Gleichungen suchen, welche aus t dadurch hervorgehen, dass man in seinem Ausdrucke für R der Reihe nach $R^2, R^3, R^4, \ldots, R^\beta$ substituiert, nämlich

$$t' = a + R^2b + R^4c + \cdots + R^{2\beta-2}m,\quad t'' = a + R^3b + R^6c + \cdots + R^{3\beta-3}m, \cdots$$

Die letzte hat man allerdings schon, da sie offenbar gleich $a + b + c + \cdots + m = (\beta\gamma, 1)$ wird; die übrigen aber können in folgender Weise abgeleitet werden: Wenn man nach den Regeln des Artikels 345, ebenso wie t^β vorher in I, das Product $t^{\beta-2}t'$ entwickelt, so beweist man auf eine der vorigen völlig analoge Art, dass das Resultat davon auf eine solche Form

$$\mathfrak{N} + \mathfrak{A}(\beta\gamma, 1) + \mathfrak{A}'(\beta\gamma, g) + \mathfrak{A}''(\beta\gamma, g^2) + \cdots = T'$$

gebracht werden kann, dass $\mathfrak{N}, \mathfrak{A}, \mathfrak{A}', \ldots$ rationale ganze Functionen von R sind und daher T' eine bekannte Grösse ist, aus der sich $t' = \frac{T't^2}{T}$ ergiebt. Wenn man ferner annimmt, dass aus der Entwicklung des Products $t^{\beta-3}t'$ die Function T'' hervorgehe, so wird in ganz derselben Weise dieser Ausdruck eine ähnliche Form annehmen und somit aus seinem bekannten Werte t'' mittelst der Gleichung $t'' = \frac{T''t^3}{T}$ sich ergeben; ebenso wird t''' durch die Gleichung $t''' = \frac{T'''t^4}{T}$, wo T''' eine bekannte Grösse ist, gefunden, u. s. w.

Diese Methode würde nicht anwendbar sein, wenn $t = 0$ werden könnte, woraus dann auch $T = T' = T'' = \cdots = 0$ sein müsste; man kann aber beweisen, dass dies unmöglich ist, wenn wir auch den Beweis seiner Weitläufigkeit wegen an dieser Stelle unterdrücken müssen. — Es giebt auch besondere Kunstgriffe, vermittelst deren die Brüche $\frac{T'}{T}$, $\frac{T''}{T}$, $\cdots$ in rationale ganze Functionen von R verwandelt werden können, sowie kürzere Methoden für den Fall $\alpha = 1$ zur Ermittlung der Werte von t', t'', ...; doch müssen wir dies Alles hier stillschweigend übergehen.

IV. Endlich hat man, sobald t, t', t'', ... gefunden sind, nach der Bemerkung III im vorigen Artikel sogleich $t + t' + t'' + \cdots = \beta a$, wonach der Wert von a bekannt ist, aus dem dann nach Artikel 346 die Werte aller übrigen Aggregate von γ Gliedern abgeleitet werden können. — Die Werte von b, c, d, ... können auch durch folgende Gleichungen erhalten werden, deren Grund jedem aufmerksamen Leser leicht ersichtlich sein wird:

$$\beta b = R^{\beta-1}\, t + R^{\beta-2}\, t' + R^{\beta-3}\, t'' + \cdots$$
$$\beta c = R^{2\beta-2} t + R^{2\beta-4} t' + R^{2\beta-6} t'' + \cdots$$
$$\beta d = R^{3\beta-3} t + R^{3\beta-6} t' + R^{3\beta-9} t'' + \cdots$$
$$\cdots\cdots\cdots\cdots\cdots$$

Aus der grossen Zahl von Bemerkungen, welche sich auf die vorstehende Untersuchung beziehen, wollen wir hier nur eine berühren. Was die Lösung der reinen Gleichung $x^\beta - T = 0$ anlangt, so ist klar, dass T in den meisten Fällen einen imaginären Wert $P + iQ$ hat, so dass jene Lösung bekanntlich teils von der Teilung eines Winkels (dessen Tangente $= \frac{Q}{P}$ ist) teils von der Teilung eines Verhältnisses (des Verhältnisses der Einheit zu $\sqrt{P^2 + Q^2}$) in β Teile abhängen wird. Dabei ist es sehr merkwürdig (was wir jedoch hier nicht ausführlicher verfolgen), dass der Wert von $\sqrt[\beta]{P^2 + Q^2}$ stets rational durch schon bekannte Grössen dargestellt werden kann, so dass ausser der Ausziehung einer Quadratwurzel zur Lösung nur die Teilung eines Winkels erforderlich ist, z. B. für $\beta = 3$ nur die Dreiteilung des Winkels.

Da endlich nichts im Wege steht, $\alpha = 1$, $\gamma = 1$ und daher $\beta = n - 1$ zu setzen, so ist klar, dass die Lösung der Gleichung $x^n - 1 = 0$ sogleich auf die Lösung einer reinen Gleichung $(n-1)^{\text{ten}}$ Grades $x^{n-1} - T = 0$, wo T durch die Wurzeln der Gleichung $x^{n-1} - 1 = 0$ bestimmt wird, reduciert werden kann. Hieraus folgt mit Hülfe der eben gemachten Bemerkung, dass die Teilung des ganzen Kreises in n gleiche Teile erfordert: 1. die Teilung des ganzen Kreises in $n - 1$ Teile; 2. die Teilung eines andern Bogens, der nach Ausführung jener Teilung construiert werden kann, in $n - 1$ Teile; 3. die Ausziehung einer einzigen Quadratwurzel, und zwar lässt sich zeigen, dass diese immer $\sqrt{n}$ ist.

Anwendung der vorstehenden Untersuchungen auf die trigonometrischen Functionen. Methode, die Winkel, welchen die einzelnen Wurzeln Ω entsprechen, zu unterscheiden.

361.

Wir haben nun noch den Zusammenhang zwischen den Wurzeln Ω und den trigonometrischen Functionen der Winkel $\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n}, \ldots, \frac{(n-1)P}{n}$ näher zu betrachten. Die Methode, welche wir für die Auffindung der Wurzeln Ω auseinandergesetzt haben, ist so beschaffen, dass sie es noch unentschieden lässt (wenn man nicht die Sinustafeln während der Rechnung in der oben beschriebenen Weise benutzt hat, was jedoch minder direct sein würde), welche Wurzel jedem einzelnen von jenen Winkeln entspricht, d. h. welche Wurzel $= \cos\frac{P}{n} + i\sin\frac{P}{n}$, welche $= \cos\frac{2P}{n} + i\sin\frac{2P}{n}$ u. s. w. ist. Diese Ungewissheit wird aber leicht entschieden, wenn man bedenkt, dass die Cosinus der Winkel $\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n}, \ldots, \frac{(n-1)P}{2n}$ beständig abnehmen (wofern man auch auf die Vorzeichen achtet), die Sinus sämtlich positiv sind, die Winkel $\frac{(n-1)P}{n}, \frac{(n-2)P}{n}, \frac{(n-3)P}{n}, \ldots, \frac{(n+1)P}{2n}$ aber respective dieselben Cosinus, aber negative, übrigens den Sinus jener an absoluter Grösse gleiche Sinus haben. Daher werden von den Wurzeln Ω diejenigen beiden, welche die grössten reellen (unter sich gleichen) Teile besitzen, den Winkeln $\frac{P}{n}, \frac{(n-1)P}{n}$ entsprechen und zwar dem ersten diejenige Wurzel, in welcher die imaginäre Grösse i mit einer positiven Grösse, dem letzteren diejenige, in welcher i mit einer negativen Grösse multipliciert ist. Von den $n-3$ übrigen Wurzeln werden wiederum diejenigen, welche die grössten reellen Teile besitzen, den Winkeln $\frac{2P}{n}, \frac{(n-2)P}{n}$ entsprechen, u. s. w. — Sobald diejenige Wurzel, welcher der Winkel $\frac{P}{n}$ entspricht, bekannt ist, können die den andern Winkeln entsprechenden Wurzeln auch dadurch unterschieden werden, dass, wenn jene $=[\lambda]$ angenommen wird, den Winkeln $\frac{2P}{n}, \frac{3P}{n}, \frac{4P}{n}, \ldots$ offenbar die Wurzeln $[2\lambda], [3\lambda], [4\lambda], \ldots$ entsprechen. So sieht man im Beispiel des Artikel 353 sofort, dass dem Winkel $\frac{1}{19}P$ keine andere Wurzel entsprechen kann als [11] und dem Winkel $\frac{18}{19}P$ keine andere als [8]; ebenso entsprechen den Winkeln $\frac{2}{19}P, \frac{17}{19}P, \frac{3}{19}P, \frac{16}{19}P, \ldots$ respective die Wurzeln [3], [16], [14], [5], ... Im Beispiel des Artikels 354 entspricht dem Winkel $\frac{1}{17}P$ offenbar die Wurzel [1], dem Winkel $\frac{2}{17}P$ die folgende [2], u. s. w. Auf diese Weise sind daher die Cosinus und Sinus der Winkel $\frac{P}{n}, \frac{2P}{n}, \ldots$ vollständig bestimmt.

Die Tangenten, Cotangenten, Sekanten und Cosekanten werden aus den Sinus und Cosinus ohne Division bestimmt.

362.

Was aber die übrigen trigonometrischen Functionen dieser Wurzeln anlangt, so könnten dieselben zwar aus den entsprechenden Sinus und Cosinus mittelst der allgemein bekannten Methoden, nämlich die Sekanten und die Tangenten, indem man die Einheit und die Sinus durch die Cosinus dividiert, ferner die Cosekanten und Cotangenten, indem man die Einheit und die Cosinus durch die Sinus dividiert, leicht abgeleitet werden. Aber bequemer wird dasselbe meistenteils mit Hülfe der folgenden Formeln ohne Divisionen durch blosse Additionen erreicht.

Es sei ω irgend einer der Winkel $\frac{P}{n}, \frac{2P}{n}, \ldots, \frac{(n-1)P}{n}$ und $\cos\omega + i\sin\omega = R$, so dass R irgend eine der Wurzeln Ω,

$$\cos\omega = \frac{1}{2}\left(R + \frac{1}{R}\right) = \frac{1+R^2}{2R}, \quad \sin\omega = \frac{1}{2i}\left(R - \frac{1}{R}\right) = i\frac{1-R^2}{2R}$$

ist. Hieraus folgt:

$$\sec\omega = \frac{2R}{1+R^2}, \quad \operatorname{tang}\omega = \frac{i(1-R^2)}{1+R^2}, \quad \operatorname{cosec}\omega = \frac{2Ri}{R^2-1}, \quad \operatorname{cotang}\omega = \frac{i(R^2+1)}{R^2-1}.$$

Wir werden nun zeigen, wie man die Zähler dieser vier Brüche so transformieren kann, dass sie durch die Nenner teilbar werden.

I. Wegen $R = R^{n+1} = R^{2n+1}$ wird $2R = R + R^{2n+1}$, welcher Ausdruck offenbar durch $1 + R^2$ teilbar ist, da n eine ungerade Zahl ist. Dadurch entsteht:

$$\sec\omega = R - R^3 + R^5 - R^7 + \cdots + R^{2n-1}$$

und daher (da wegen $\sin\omega = -\sin(2n-1)\omega$, $\sin 3\omega = -\sin(2n-3)\omega, \ldots$ offenbar $\sin\omega - \sin 3\omega + \sin 5\omega - \cdots + \sin(2n-1)\omega = 0$ ist)

$$\sec\omega = \cos\omega - \cos 3\omega + \cos 5\omega - \cdots + \cos(2n-1)\omega$$

oder endlich (da $\cos\omega = \cos(2n-1)\omega$, $\cos 3\omega = \cos(2n-3)\omega, \ldots$ ist):

$$\sec\omega = 2[\cos\omega - \cos 3\omega + \cos 5\omega - \cdots \mp \cos(n-2)\omega] \pm \cos n\omega,$$

wo das obere oder untere Zeichen gilt, je nachdem n von der Form $4k+1$ oder von der Form $4k+3$ ist. Offenbar kann diese Formel auch so dargestellt werden:

$$\sec\omega = \pm[1 - 2\cos 2\omega + 2\cos 4\omega - \cdots \pm 2\cos(n-1)\omega].$$

II. Substituiert man in ähnlicher Weise $1 - R^{2n+2}$ für $1 - R^2$, so ergiebt sich:

$$\operatorname{tang}\omega = i(1 - R^2 + R^4 - R^6 + \cdots - R^{2n})$$

oder (da $1 - R^{2n} = 0$, $R^2 - R^{2n-2} = 2i \sin 2\omega$, $R^4 - R^{2n-4} = 2i \sin 4\omega, \ldots$ ist):

$$\operatorname{tang}\omega = 2[\sin 2\omega - \sin 4\omega + \sin 6\omega - \cdots \mp \sin(n-1)\omega].$$

III. Da man $1 + R^2 + R^4 + \cdots + R^{2n-2} = 0$ hat, so folgt:

$$n = n - 1 - R^2 - R^4 - \cdots - R^{2n-2} = (1-1) + (1-R^2) + (1-R^4) + \cdots + (1 - R^{2n-2}),$$

und die einzelnen Teile dieses Aggregats sind durch $1 - R^2$ teilbar. Hiernach wird:

$$\frac{n}{1-R^2} = 1 + (1 + R^2) + (1 + R^2 + R^4) + \cdots + (1 + R^2 + R^4 + \cdots + R^{2n-4})$$
$$= (n-1) + (n-2)R^2 + (n-3)R^4 + \cdots + R^{2n-4},$$

somit, wenn man mit 2 multipliciert, sodann hiervon

$$0 = (n-1)(1 + R^2 + R^4 + \cdots + R^{2n-2})$$

subtrahiert und wiederum mit R multipliciert:

$$\frac{2nR}{1-R^2} = (n-1)R + (n-3)R^3 + (n-5)R^5 + \cdots - (n-3)R^{2n-3} - (n-1)R^{2n-1},$$

woraus sogleich folgt:

$$\operatorname{cosec}\omega = \frac{1}{n}[(n-1)\sin\omega + (n-3)\sin 3\omega + \cdots - (n-1)\sin(2n-1)\omega]$$
$$= \frac{2}{n}[(n-1)\sin\omega + (n-3)\sin 3\omega + \cdots + 2\sin(n-2)\omega],$$

und diese Formel kann auch so dargestellt werden:

$$\operatorname{cosec}\omega = -\frac{2}{n}[2\sin 2\omega + 4\sin 4\omega + 6\sin 6\omega + \cdots + (n-1)\sin(n-1)\omega]$$

IV. Multipliciert man den oben angegebenen Wert von $\frac{n}{1-R^2}$ mit $1 + R^2$ und subtrahiert davon

$$0 = (n-1)(1 + R^2 + R^4 + \cdots + R^{2n-2}),$$

so entsteht

$$\frac{n(1+R^2)}{1-R^2} = (n-2)R^2 + (n-4)R^4 + (n-6)R^6 + \cdots - (n-2)R^{2n-2},$$

woraus sogleich folgt:

$$\begin{aligned}\operatorname{cotang}\omega &= \frac{1}{n}[(n-2)\sin 2\omega + (n-4)\sin 4\omega + (n-6)\sin 6\omega + \cdots \\ &\qquad - (n-2)\sin(n-2)\omega] \\ &= \frac{2}{n}[(n-2)\sin 2\omega + (n-4)\sin 4\omega + \cdots + 3\sin(n-3)\omega \\ &\qquad + \sin(n-1)\omega],\end{aligned}$$

und diese Formel kann man auch in folgender Weise darstellen:

$$\operatorname{cotang}\omega = -\frac{2}{n}[\sin\omega + 3\sin 3\omega + \cdots + (n-2)\sin(n-2)\omega]$$

Methode, die Gleichungen für die trigonometrischen Functionen allmälig zu erniedrigen.

363.

Ebenso wie unter der Annahme, dass $n-1=ef$ sei, die Function X in e Factoren von f Dimensionen zerlegt werden kann, sobald die Werte sämtlicher e Aggregate von f Gliedern bekannt sind (Artikel 348), so lässt sich auch dann, wenn man annimmt, dass $Z=0$ die Gleichung $(n-1)^{\text{ten}}$ Grades ist, deren Wurzeln die Sinus oder irgendwelche andere trigonometrischen Functionen der Winkel $\frac{P}{n}, \frac{2P}{n}, \ldots, \frac{(n-1)P}{n}$ sind, die Function Z in e Factoren von f Dimensionen zerlegen. Die Hauptmomente für ein solches Verfahren sind folgende:

Es bestehe Ω aus den folgenden e Perioden von f Gliedern $(f, 1)=P$, P', P'', ..., und die Periode P aus den Wurzeln [1], $[a]$, $[b]$, $[c]$, ..., P' aus den Wurzeln $[a']$, $[b']$, $[c']$, ..., P'' aus $[a'']$, $[b'']$, $[c'']$, ... Es entspreche ferner der Wurzel [1] der Winkel ω und daher den Wurzeln $[a]$, $[b]$, ..., die Winkel $a\omega$, $b\omega$, ..., den Wurzeln $[a']$, $[b']$, ... die Winkel $a'\omega$, $b'\omega$, ..., den Wurzeln $[a'']$, $[b'']$, $[c'']$, ... die Winkel $a''\omega$, $b''\omega$, ..., u. s. w. Dann sieht man leicht, dass alle diese Winkel zusammengenommen mit den Winkeln $\frac{P}{n}, \frac{2P}{n}, \frac{3P}{n}, \ldots, \frac{(n-1)P}{n}$ hinsichtlich ihrer trigonometrischen Functionen*) übereinstimmen. Wenn daher

*) In dieser Hinsicht stimmen zwei Winkel überein, deren Differenz entweder der ganzen Peripherie oder irgend einem Vielfachen derselben gleich ist; derartige Winkel könnten wir nach der Peripherie congruent nennen, wenn man die Congruenz iu etwas weiterem Sinne verstehen wollte.

die in Rede stehende Function durch den dem Winkel vorgesetzten Buchstaben φ bezeichnet wird, und man das Product aus den Factoren

$$x - \varphi(\omega), \quad x - \varphi(a\omega), \quad x - \varphi(b\omega), \ldots$$

gleich Y, das Product aus den Factoren $x - \varphi(a'\omega)$, $x - \varphi(b'\omega), \ldots$ gleich Y', das Product aus den Factoren $x - \varphi(a''\omega)$, $x - \varphi(b''\omega)$, $x - \varphi(c''\omega), \ldots$ gleich Y'', u. s. w. setzt, so wird offenbar das Product $YY'Y'' \ldots = Z$. Wir haben nur noch zu zeigen, dass sämtliche Coefficienten in den Functionen $Y, Y', Y'', \ldots$ auf eine solche Form:

$$A + B(f, 1) + C(f, g) + D(f, g^2) + \cdots + L(f, g^{e-1})$$

gebracht werden kann, wonach offenbar alle für bekannt zu betrachten sein werden, sobald die Werte aller Aggregate von f Gliedern bekannt sind. Dies erreichen wir auf folgende Weise:

Ebenso wie $\cos\omega = \frac{1}{2}[1] + \frac{1}{2}[1]^{n-1}$, $\sin\omega = -\frac{1}{2}i[1] + \frac{1}{2}i[1]^{n-1}$ ist, so können auch die übrigen trigonometrischen Functionen des Winkels ω auf eine solche Form $\mathfrak{A} + \mathfrak{B}[1] + \mathfrak{C}[1]^2 + \mathfrak{D}[1]^3 + \cdots$ reduciert werden, und es ist ohne Weiteres ersichtlich, dass die Functionen des Winkels $k\omega$ alsdann werden $\mathfrak{A} + \mathfrak{B}[k] + \mathfrak{C}[k]^2 + \mathfrak{D}[k]^3 + \cdots$, wo k irgend eine ganze Zahl bezeichnet. Da nun die einzelnen Coefficienten in Y rationale ganze symmetrische Functionen von $\varphi(\omega)$, $\varphi(a\omega)$, $\varphi(b\omega), \ldots$ sind, so ist klar, dass, wenn für diese Grössen ihre Werte substituiert werden, die einzelnen Coefficienten rationale ganze symmetrische Functionen von $[1]$, $[a]$, $[b], \ldots$ werden, weshalb sie sich nach Artikel 347 auf die Form $A + B(f, 1) + C(f, g) + \cdots$ reducieren. Und aus ganz demselben Grunde wird es auch möglich sein, sämtliche Coefficienten in Y', $Y'', \ldots$ auf eine ähnliche Form zu reducieren.

364.

In Bezug auf das Problem des vorigen Artikels fügen wir noch einige Bemerkungen hinzu.

I. Da die einzelnen Coefficienten in Y' ebensolche Functionen von den in der Periode P' (die wir gleich (f, a') setzen dürfen) enthaltenen Wurzeln sind, wie die entsprechenden Coefficienten in P Functionen von den Wurzeln in P sind, so geht aus Artikel 347 hervor, dass Y' aus Y abgeleitet werden kann, wenn man nur überall in Y für $(f, 1)$, (f, g), $(f, g^2), \ldots$ bezüglich (f, a'), $(f, a'g)$, $(f, a'g^2), \ldots$ substituiert. Und ebenso wird Y'' aus Y abgeleitet werden, wenn man überall in Y für $(f, 1)$, (f, g), $(f, g^2), \ldots$ respective (f, a''), $(f, a''g)$, $(f, a''g^2), \ldots$ substituiert. Sobald daher die Function Y entwickelt ist, so folgen die übrigen Y', $Y'', \ldots$ daraus ohne Weiteres.

II. Nimmt man

$$Y = x^f - \alpha x^{f-1} + \beta x^{f-2} - \cdots.$$

an, so sind die Coefficienten $\alpha, \beta, \ldots$ respective die Summe der Wurzeln der Gleichung $Y=0$, d. i. der Grössen $\varphi(\omega)$, $\varphi(a\omega)$, $\varphi(b\omega)\ldots$, die Summe der Producte aus je zweien von diesen Grössen, u. s. w. Meistenteils aber werden diese Coefficienten viel bequemer durch eine, der im Artikel 349 angegebenen ähnliche Methode gefunden, indem man die Summe der Wurzeln $\varphi(\omega)$, $\varphi(a\omega)$, $\varphi(b\omega), \ldots$, die Summe der Quadrate, der Kuben, u. s. w. berechnet und daraus nach dem Newton'schen Satze jene Coefficienten ableitet. — So oft φ die Tangente, Sekante, Cotangente oder Cosekante bezeichnet, giebt es noch andere Hülfsmittel, die wir aber hier mit Stillschweigen übergehen.

III. Eine besondere Betrachtung verdient der Fall, wo f eine gerade Zahl ist, und daher jede Periode $P, P', P'', \ldots$ aus $\frac{1}{2}f$ Perioden von je zwei Gliedern zusammengesetzt ist. Besteht P aus den Perioden $(2, 1)$, $(2, \mathfrak{a})$, $(2, \mathfrak{b})$, $(2, \mathfrak{c})$, $\ldots$, so werden die Zahlen $1, \mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$ und $n-1$, $n-\mathfrak{a}$, $n-\mathfrak{b}$, $n-\mathfrak{c}$, $\ldots$ zusammengenommen mit den Zahlen $1, a, b, c, \ldots$ übereinstimmen oder wenigstens (was hier auf dasselbe hinauskommt) diesen nach dem Modul n congruent sein. Es ist aber $\varphi\big((n-1)\omega\big) = \pm\varphi(\omega)$, $\varphi\big((n-\mathfrak{a})\omega\big) = \pm\varphi(\mathfrak{a}\omega)$, u. s. w., wo die oberen Zeichen gelten, wenn φ den Cosinus oder die Sekante, die unteren, wenn φ den Sinus, die Tangente, Cotangente oder Cosekante bezeichnet. Hieraus folgt, dass in den beiden ersteren Fällen unter den Factoren, aus denen Y besteht, stets je zwei gleich sind und daher Y ein Quadrat ist, und zwar $Y=y^2$, wenn y gleich dem Producte aus

$$x-\varphi(\omega),\quad x-\varphi(\mathfrak{a}\omega),\quad x-\varphi(\mathfrak{b}\omega),\ \ldots$$

gesetzt wird. Ebenso sind in denselben Fällen die übrigen Functionen Y', Y'', $\ldots$ Quadrate, und zwar wird, wenn man annimmt, dass P' aus $(2, \mathfrak{a}')$, $(2, \mathfrak{b}')$, $(2, \mathfrak{c}')$, $\ldots$, P'' aus $(2, \mathfrak{a}'')$, $(2, \mathfrak{b}'')$, $(2, \mathfrak{c}'')$, $\ldots$, u. s. w. bestehe und dass das Product aus $x-\varphi(\mathfrak{a}'\omega)$, $x-\varphi(\mathfrak{b}'\omega)$, $x-\varphi(\mathfrak{c}'\omega)$, $\ldots$ gleich y', das Product aus $x-\varphi(\mathfrak{a}''\omega)$, $x-\varphi(\mathfrak{b}''\omega)$, $\ldots$ gleich y'' ist, u. s. w., $Y'=y'^2$, $Y''=y''^2$, u. s. w. Ferner ist auch die Function Z ein Quadrat (vgl. oben Artikel 337) und die Wurzel desselben dem Producte aus $yy'y''$, $\ldots$ gleich. Übrigens sieht man leicht, dass $y', y'', \ldots$ ebenso aus y abgeleitet werden, wie $Y', Y'', \ldots$ nach dem in I Gesagten aus Y sich ergeben; sowie ferner, dass die einzelnen Coefficienten in y auch auf die Form

$$A + B(f, 1) + C(f, g) + \cdots$$

reduciert werden können, da die Summen der einzelnen Potenzen der Wurzeln der Gleichung $y=0$ offenbar die Hälften der Potenzen der Wurzeln der Gleichung $Y=0$ und daher auf eine solche Form reducierbar sind. In den vier letzteren Fällen aber ist Y das Product aus den Factoren

$$x^2-\big(\varphi(\omega)\big)^2,\quad x^2-\big(\varphi(\mathfrak{a}\omega)\big)^2,\quad x^2-\big(\varphi(\mathfrak{b}\omega)\big)^2,\ \ldots$$

und daher von der Form:

$$x^f - \lambda x^{f-2} + \mu x^{f-4} - \ldots,$$

und es ist klar, dass die Coefficienten λ, μ, ... sich aus den Summen der Quadrate, Biquadrate, u. s. w. der Wurzeln $\varphi(\omega)$, $\varphi(\mathfrak{a}\omega)$, $\varphi(\mathfrak{b}\omega)$, ... herleiten lassen, und ebenso verhalten sich die Functionen Y', Y'', ...

Beispiel I. Es sei $n = 17$, $f = 8$ und es bezeichne φ den Cosinus. Hieraus wird:

$$Z = \left(x^8 + \frac{1}{2}x^7 - \frac{7}{4}x^6 - \frac{3}{4}x^5 + \frac{15}{16}x^4 + \frac{5}{16}x^3 - \frac{5}{32}x^2 - \frac{1}{32}x + \frac{1}{256}\right)^2,$$

und man hat demnach $\sqrt{Z}$ in zwei Factoren von je vier Dimensionen y, y' zu zerlegen. Die Periode $P = (8, 1)$ besteht aus $(2, 1)$, $(2, 9)$, $(2, 13)$, $(2, 15)$, daher wird y das Product aus den Factoren:

$$x - \varphi(\omega), \quad x - \varphi(9\omega), \quad x - \varphi(13\omega), \quad x - \varphi(15\omega).$$

Substituiert man $\frac{1}{2}[k] + \frac{1}{2}[n-k]$ für $\varphi(k\omega)$, so findet man:

$$\varphi(\omega) + \varphi(9\omega) + \varphi(13\omega) + \varphi(15\omega) = \tfrac{1}{2}(8, 1);$$
$$\big(\varphi(\omega)\big)^2 + \big(\varphi(9\omega)\big)^2 + \big(\varphi(13\omega)\big)^2 + \big(\varphi(15\omega)\big)^2 = 2 + \tfrac{1}{4}(8, 1);$$

ebenso die Summe der Kuben gleich $\frac{3}{8}(8, 1) + \frac{1}{8}(8, 3)$, die Summe der Biquadrate gleich $1\frac{1}{2} + \frac{5}{16}(8, 1)$. Werden hieraus nach dem Newton'schen Satze die Coefficienten in y bestimmt, so ergiebt sich:

$$y = x^4 - \frac{1}{2}(8, 1)x^3 + \frac{1}{4}[(8, 1) + 2(8, 3)]x^2 - \frac{1}{8}[(8, 1) + 3(8, 3)]x + \frac{1}{16}[(8, 1) + (8, 3)];$$

y' aber geht aus y hervor, wenn man $(8, 1)$ mit $(8, 3)$ vertauscht. Substituiert man also für $(8, 1)$, $(8, 3)$ die Werte $-\frac{1}{2} + \frac{1}{2}\sqrt{17}$, $-\frac{1}{2} - \frac{1}{2}\sqrt{17}$, so folgt:

$$y = x^4 + \left(\frac{1}{4} - \frac{1}{4}\sqrt{17}\right)x^3 - \left(\frac{3}{8} + \frac{1}{8}\sqrt{17}\right)x^2 + \left(\frac{1}{4} + \frac{1}{8}\sqrt{17}\right)x - \frac{1}{16}$$
$$y' = x^4 + \left(\frac{1}{4} + \frac{1}{4}\sqrt{17}\right)x^3 - \left(\frac{3}{8} - \frac{1}{8}\sqrt{17}\right)x^2 + \left(\frac{1}{4} - \frac{1}{8}\sqrt{17}\right)x - \frac{1}{16}.$$

Auf ähnliche Weise kann $\sqrt{Z}$ in vier Factoren von je zwei Dimensionen zerlegt werden, von denen der erste $\big(x - \varphi(\omega)\big)\big(x - \varphi(13\omega)\big)$, der zweite $\big(x - \varphi(9\omega)\big)\big(x - \varphi(15\omega)\big)$, der dritte $\big(x - \varphi(3\omega)\big)\big(x - \varphi(5\omega)\big)$ und der vierte $\big(x - \varphi(10\omega)\big)\big(x - \varphi(11\omega)\big)$ ist, und alle Coefficienten in diesen

Factoren können durch die vier Aggregate (4, 1), (4, 9), (4, 3), (4, 10) ausgedrückt werden. Offenbar aber wird das Product aus dem ersten und zweiten Factor gleich y, das Product aus dem dritten und vierten Factor gleich y' sein.

Beispiel II. Wenn φ, während alles Übrige ungeändert bleibt, den Sinus bezeichnen soll, so dass

$$Z = x^{16} - \frac{17}{4}x^{14} + \frac{119}{16}x^{12} - \frac{221}{32}x^{10} + \frac{935}{256}x^{8} - \frac{561}{512}x^{6} + \frac{357}{2048}x^{4} - \frac{51}{4096}x^{2} + \frac{17}{65536}$$

in zwei Factoren y, y' von acht Dimensionen zu zerlegen ist, so ist y das Product aus den vier doppelten Factoren:

$$x^2 - \big(\varphi(\omega)\big)^2,\quad x^2 - \big(\varphi(9\omega)\big)^2,\quad x^2 - \big(\varphi(13\omega)\big)^2,\quad x^2 - \big(\varphi(15\omega)\big)^2.$$

Da nun $\varphi(k\omega) = -\frac{1}{2}i[k] + \frac{1}{2}i[n-k]$ ist, so wird

$$\big(\varphi(k\omega)\big)^2 = -\tfrac{1}{4}[2k] + \tfrac{1}{2}[n] - \tfrac{1}{4}[2n-2k] = \tfrac{1}{2} - \tfrac{1}{4}[2k] - \tfrac{1}{4}[2n-2k].$$

Hieraus findet man für die Summe der Quadrate der Wurzeln $\varphi(\omega)$, $\varphi(9\omega)$, $\varphi(13\omega)$, $\varphi(15\omega)$ den Wert: $2 - \frac{1}{4}(8,1)$, für die Summe ihrer Biquadrate: $\frac{3}{2} - \frac{3}{16}(8,1)$, für die Summe ihrer sechsten Potenzen: $\frac{5}{4} - \frac{9}{64}(8,1) - \frac{1}{64}(8,3)$, für die Summe ihrer achten Potenzen: $\frac{35}{32} - \frac{27}{256}(8,1) - \frac{1}{32}(8,3)$.

Hieraus folgt:

$$y = x^8 - \left[2 - \frac{1}{4}(8,1)\right]x^6 + \left[\frac{3}{2} - \frac{5}{16}(8,1) + \frac{1}{8}(8,3)\right]x^4 - \left[\frac{1}{2} - \frac{9}{64}(8,1) + \frac{5}{64}(8,3)\right]x^2 + \frac{1}{16} - \frac{5}{256}(8,1) + \frac{3}{256}(8,3),$$

und y' geht aus y hervor, wenn man (8, 1) und (8, 3) mit einander vertauscht, so dass man durch Substitution der Werte dieser Aggregate erhält:

$$y = x^8 - \left(\frac{17}{8} - \frac{1}{8}\sqrt{17}\right)x^6 + \left(\frac{51}{32} - \frac{7}{32}\sqrt{17}\right)x^4 - \left(\frac{17}{32} - \frac{7}{64}\sqrt{17}\right)x^2 + \frac{17}{256} - \frac{1}{64}\sqrt{17}$$

$$y' = x^8 - \left(\frac{17}{8} + \frac{1}{8}\sqrt{17}\right)x^6 + \left(\frac{51}{32} + \frac{7}{32}\sqrt{17}\right)x^4 - \left(\frac{17}{32} + \frac{7}{64}\sqrt{17}\right)x^2 + \frac{17}{256} + \frac{1}{64}\sqrt{17}.$$

Ebenso lässt sich Z in vier Factoren zerlegen, deren Coefficienten durch die Aggregate von vier Gliedern ausgedrückt werden können, und zwar ist das Product aus zweien gleich y, das Product aus den beiden übrigen gleich y'.

Die Teilungen des Kreises, welche man mittelst quadratischer Gleichungen oder durch geometrische Constructionen ausführen kann.

365.

Wir haben somit durch die vorstehenden Untersuchungen die Teilung des Kreises in n gleiche Teile, wenn n eine Primzahl ist, auf die Auflösung von so vielen Gleichungen zurückgeführt, als die Anzahl der Factoren beträgt, in welche man die Zahl $n-1$ zerlegen kann, und zwar bestimmt sich der Grad dieser Gleichungen durch die Grösse der Factoren. So oft daher $n-1$ eine Potenz von 2 ist, was für die folgenden Werte von n der Fall ist: $n = 3, 5, 17, 257, 65537, \ldots$, lässt sich die Teilung des Kreises auf lauter quadratische Gleichungen zurückführen, und die trigonometrischen Functionen der Winkel $\frac{P}{n}, \frac{2P}{n}, \ldots$ lassen sich durch mehr oder weniger complicierte (je nach der Grösse von n) quadratische Gleichungen ausdrücken. Daher kann in diesen Fällen die Teilung des Kreises in n gleiche Teile oder die Beschreibung eines regulären Polygons von n Seiten durch geometrische Constructionen erledigt werden. Z. B. leitet man für $n = 17$ aus den Artikeln 354, 361 für den Cosinus des Winkels $\frac{1}{17}P$ leicht den folgenden Ausdruck her:

$$-\frac{1}{16}+\frac{1}{16}\sqrt{17}+\frac{1}{16}\sqrt{34-2\sqrt{17}}$$
$$+\frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}};$$

die Cosinus der Vielfachen jenes Winkels haben eine ähnliche Form, die Sinus aber haben ein Wurzelzeichen mehr. Es ist sicherlich sehr merkwürdig, dass, während schon zu Euclid's Zeiten die geometrische Teilbarkeit des Kreises in drei und fünf Teile bekannt war, diesen Entdeckungen im Verlauf von 2000 Jahren nichts hinzugefügt worden ist, und dass es sämtliche Geometer für sicher erklärten, dass sich ausser jenen Teilungen und denen, die ohne Weiteres daraus sich ergeben, nämlich den Teilungen in 15, $3 \cdot 2^\mu$, $5 \cdot 2^\mu$, $15 \cdot 2^\mu$ sowie in 2^μ Teile, keine andern weiter durch geometrische Constructionen ausführen lassen. — Übrigens beweist man leicht, dass, wenn die Primzahl $n = 2^m + 1$ ist, auch der Exponent m keine andern Primfactoren haben darf, als die Zahl 2, und daher entweder gleich

1 oder gleich 2 oder gleich einer höheren Potenz von 2 sein muss; denn wenn m durch irgend eine ungerade Zahl ζ (welche grösser als 1 ist) teilbar und $m = \zeta\eta$ wäre, so würde $2^m + 1$ durch $2^\eta + 1$ teilbar und daher eine zusammengesetzte Zahl sein. Alle Werte von n also, für welche wir bloss zu quadratischen Gleichungen gelangen, sind unter der Form $2^{2^\nu} + 1$ enthalten; auf diese Weise ergeben sich die fünf Zahlen 3, 5, 17, 257, 65537, wenn man $\nu = 0, 1, 2, 3, 4$ oder $m = 1, 2, 4, 8, 16$ setzt. Keineswegs aber lässt sich für alle unter jener Form enthaltenen Zahlen die Teilung des Kreises geometrisch durchführen, sondern nur für diejenigen, welche Primzahlen sind. Zwar hatte Fermat, durch Induction irregeführt, behauptet, dass alle unter jener Form enthaltenen Zahlen notwendig Primzahlen seien; indessen hat Euler zuerst bemerkt, dass jene Regel schon für $\nu = 5$ oder $m = 32$ falsch ist, da die Zahl $2^{32} + 1 = 4294967297$ den Factor 641 enthält.

So oft aber $n - 1$ andere Primfactoren ausser 2 enthält, gelangen wir immer zu höheren Gleichungen, nämlich zu einer oder mehreren kubischen, wenn 3 einmal oder mehrere Male unter den Primfactoren von $n - 1$ vorkommt, zu Gleichungen fünften Grades, wenn $n - 1$ durch 5 teilbar ist, u. s. w., und wir können mit aller Strenge beweisen, dass diese höheren Gleichungen **durchaus nicht vermieden oder auf Gleichungen von niedrigerem Grade zurückgeführt werden können**; obwohl die Grenzen dieses Werkes nicht gestatten, diesen Beweis hier mitzuteilen, glaubten wir doch darauf hinweisen zu müssen, damit nicht einer noch andere Teilungen ausser den von unserer Theorie gelieferten, z. B. die Teilungen in 7, 11, 13, 19, ... Teile auf geometrische Constructionen zurückzuführen hoffe und seine Zeit unnütz vergeude.

366.

Wenn der Kreis in a^α Teile zu teilen ist, wo a eine Primzahl bezeichnet, so kann man dies offenbar geometrisch durchführen, wenn $a = 2$ ist, aber für keinen andern Wert von a weiter, wofern $\alpha > 1$ ist; denn dann müsste man ausser denjenigen Gleichungen, welche zur Teilung in a Teile erforderlich sind, notwendig noch $\alpha - 1$ andere vom a^{ten} Grade lösen; auch diese kann man in keiner Weise vermeiden oder erniedrigen. Die Grade der notwendigen Gleichungen können also aus den Primfactoren der Zahl $(a-1)a^{\alpha-1}$ allgemein (nämlich auch für den Fall, wo $\alpha = 1$ ist) erkannt werden.

Wenn schliesslich der Kreis in $N = a^\alpha b^\beta c^\gamma \dots$ Teile geteilt werden soll, wo $a, b, c \dots$ ungleiche Primzahlen bezeichnen, so genügt es die Teilungen in $a^\alpha, b^\beta, c^\gamma, \dots$ Teile ausgeführt zu haben (Artikel 336); um daher die Grade der zu diesem Zwecke erforderlichen Gleichungen kennen zu lernen, muss man die Primfactoren der Zahlen

$$(a-1)\,a^{\alpha-1},\ (b-1)\,b^{\beta-1},\ (c-1)\,c^{\gamma-1}, \dots,$$

oder, was hier auf dasselbe hinauskommt, des Products aus diesen Zahlen betrachten. Man bemerke, dass dieses Product die Anzahl der Zahlen dar-

stellt, welche prim zu N und kleiner als N sind (Artikel 38). Geometrisch lässt sich also die Teilung nur dann ausführen, wenn diese Zahl eine Potenz von 2 ist; wenn sie aber noch andere Primfactoren ausser 2, z. B. $p, p', \ldots$ enthält, so lassen sich die Gleichungen vom p^{ten}, p'^{ten}, u. s. w. Grade in keiner Weise vermeiden. Hieraus schliesst man allgemein, dass, damit der Kreis geometrisch in N Teile geteilt werden könne, N entweder 2 oder eine höhere Potenz von 2, oder eine Primzahl von der Form $2^m + 1$ oder das Product aus mehreren solchen Primzahlen, oder das Product aus einer oder mehreren solchen Primzahlen mit 2 oder einer höheren Potenz von 2 sein muss; oder kürzer, es ist erforderlich, dass N weder irgend einen ungeraden Primfactor, welcher nicht von der Form $2^m + 1$ ist, noch auch irgend einen Primfactor von der Form $2^m + 1$ mehrmals enthalte. Solcher Werte von N findet man unterhalb 300 folgende 38: 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272.*)

*) Wären alle Zahlen von der Form $2^{2^m}+1$ Primzahlen, so würde ein hinlänglich genäherter Ausdruck für die Menge der in Rede stehenden Zahlen (N) kleiner als die gegebene Zahl M folgender sein $\frac{1}{2}\left(\frac{\log M}{\log 2}\right)^2$.

Zusätze.

Zu Artikel 28. Die Lösung der unbestimmten Gleichung $ax = by \pm 1$ ist nicht zuerst von Euler (wie dort gesagt ist), sondern schon von einem Geometer des siebzehnten Jahrhunderts, Bachet de Meziriac, dem berühmten Herausgeber und Commentator von Diophant, durchgeführt worden, und hat ihm Lagrange diese Ehre zuerkannt (*Add. à l'Algèbre d'Euler p. 525*, wo zugleich die Art des Verfahrens angegeben ist). Bachet hat seine Entdeckung in der zweiten Ausgabe seines Buches *Problèmes plaisans et délectables qui se font par les nombres 1624* mitgeteilt; in der ersten Auflage (Lyon 1612), welche ich allein einsehen konnte, findet sie sich noch nicht, obwohl sie bereits angekündigt wird.

Zu Artikel 151, 296, 297. Legendre hat seinen Beweis von neuem dargelegt in seinem herrlichen Werke *Essai d'une théorie des nombres p. 214 u. ff.*, jedoch so, dass nichts Wesentliches daran geändert ist; daher bleibt diese Methode auch noch allen im Artikel 297 gegen sie erhobenen Einwürfen ausgesetzt. Allerdings ist der Satz (auf welchen die eine Annahme sich stützt), dass sich in jeder arithmetischen Reihe l, $l + k$, $l + 2k$, ... Primzahlen finden, wenn k und l keinen gemeinschaftlichen Teiler haben, in diesem Werke weitläufiger betrachtet worden, S. 12 u. ff., doch scheint der geometrischen Strenge noch nicht Genüge gethan zu sein. Aber auch dann, wenn dieser Satz vollständig bewiesen ist, bleibt die eine Annahme übrig (dass es Primzahlen von der Form $4n + 3$ giebt, deren quadratischer Nichtrest eine gegebene Primzahl von der Form $4n + 1$, positiv genommen, ist), und ich weiss nicht, ob man denselben streng beweisen kann, ohne das Fundamentaltheorem selbst schon vorauszusetzen. Übrigens muss man bemerken, dass Legendre diese letztere Annahme nicht stillschweigend gemacht hat, sondern dass sie auch ihm selbst nicht entgangen ist, S. 221.

Zu Artikel 288—293. Über denselben Gegenstand, der hier als besondere Anwendung der Theorie der ternären Formen dargestellt ist, und der in Bezug auf Strenge und Allgemeinheit so vollkommen sein dürfte, dass nichts mehr zu wünschen übrig bleibt, hat Legendre im dritten Abschnitt

seines Werkes S. 321—400 eine viel ausführlichere Untersuchung angestellt.*) Er bediente sich dabei von den unsrigen völlig verschiedener Prinzipien und Methoden; indessen ist er auf diesem Wege in mehrere Schwierigkeiten verwickelt worden, welche bewirkten, dass er die Hauptsätze nicht durch einen strengen Beweis zu begründen vermochte. Diese Schwierigkeiten deutete er selbst in ehrlicher Weise an; aber dieselben dürften, wenn wir nicht irren, leichter beseitigt werden können als die, dass auch bei dieser Untersuchung das eben erwähnte Theorem (In jeder arithmetischen Progression u. s. w.) vorausgesetzt ist, Seite 371, Anm. am Schluss.

Zu Artikel 306 VIII. In dem dritten Tausend negativer Determinanten sind 37 irreguläre gefunden worden, von denen 18 den Irregularitäts-Exponenten 2, die 19 übrigen den Irregularitäts-Exponenten 3 haben.

Zu ebendemselben Artikel X. Es ist uns neulich geglückt, die hier gestellte Aufgabe vollständig zu lösen; diese Untersuchung, welche über mehrere Teile sowohl der höheren Arithmetik als auch der Analysis in erstaunlicher Weise Licht verbreitet, werden wir sobald als möglich in der Fortsetzung dieses Werkes mitteilen. Dieselbe hat ergeben, dass der Coefficient m im Artikel 304 gleich $\gamma\pi = 2{,}3458847616$ ist, wo γ dieselbe Grösse wie im Artikel 302 und π, wie eben dort, den halben Umfang eines Kreises vom Radius 1 bezeichnet.

---

*) Auch ohne dass wir darauf hinweisen, werden die Leser sich hüten, unsere ternären Formen mit dem zu verwechseln, was Legendre eine *forme trinaire d'un nombre* genannt hat. Mit diesem Ausdruck bezeichnete er nämlich die Zerlegung einer Zahl in drei Quadrate.

Tafel I (Artikel 58, 91).

		2. 3. 5. 7. 11.	13. 17. 19. 23. 29.	31. 37. 41. 43. 47.	53. 59. 61. 67. 71.	73. 79. 83. 89.
3	2	1.				
5	2	1. 3.				
7	3	2. 1. 5.				
9	2	1. *. 5. 4.				
11	2	1. 8. 4. 7.				
13	6	5. 8. 9. 7. 11.				
16	5	*. 3. 1. 2. 1.	3.			
17	10	10. 11. 7. 9. 13.	12.			
19	10	17. 5. 2. 12. 6.	13. 8.			
23	10	8. 20. 15. 21. 3.	12. 17. 5.			
25	2	1. 7. *. 5. 16.	19. 13. 18. 11.			
27	2	1. *. 5. 16. 13.	8. 15. 12. 11.			
29	10	11. 27. 18. 20. 23.	2. 7. 15. 24.			
31	17	12. 13. 20. 4. 29.	23. 1. 22. 21. 27.			
32	5	*. 3. 1. 2. 5.	7. 4. 7. 6. 3.	0.		
37	5	11. 34. 1. 28. 6.	13. 5. 25. 21. 15.	27.		
41	6	26. 15. 22. 39. 3.	31. 33. 9. 36. 7.	28. 32.		
43	28	39. 17. 5. 7. 6.	40. 16. 29. 20. 25.	32. 35. 18.		
47	10	30. 18. 17. 38. 27.	3. 42. 29. 39. 43.	5. 24. 25. 37.		
49	10	2. 13. 41. *. 16.	9. 31. 35. 32. 24.	7. 38. 27. 36. 23.		
53	26	25. 9. 31. 38. 46.	28. 42. 41. 39. 6.	45. 22. 33. 30. 8.		
59	10	25. 32. 34. 44. 45.	23. 14. 22. 27. 4.	7. 41. 2. 13. 53.	28.	
61	10	47. 42. 14. 23. 45.	20. 49. 22. 39. 25.	13. 33. 18. 41. 40.	51. 17.	
64	5	*. 3. 1. 10. 5.	15. 12. 7. 14. 11.	8. 9. 14. 13. 12.	5. 1. 3.	
67	12	29. 9. 39. 7. 61.	23. 8. 26. 20. 22.	43. 44. 19. 63. 64.	3. 54. 5.	
71	62	58. 18. 14. 33. 43.	27. 7. 38. 5. 4.	13. 30. 55. 44. 17.	59. 29. 37. 11.	
73	5	8. 6. 1. 33. 55.	59. 21. 62. 46. 35.	11. 64. 4. 51. 31.	53. 5. 58. 50. 44.	
79	29	50. 71. 34. 19. 70.	74. 9. 10. 52. 1.	76. 23. 21. 47. 55.	7. 17. 75. 54. 33.	4.
81	11	25. *. 35. 22. 1.	38. 15. 12. 5. 7.	14. 24. 29. 10. 13.	45. 53. 4. 20. 33.	48. 52.
83	50	3. 52. 81. 24. 72.	67. 4. 59. 16. 36.	32. 60. 38. 49. 69.	13. 20. 34. 53. 17.	43. 47.
89	30	72. 87. 18. 7. 4.	65. 82. 53. 31. 29.	57. 77. 67. 59. 34.	10. 45. 19. 32. 26.	68. 46. 27.
97	10	86. 2. 11. 53. 82.	83. 19. 27. 79. 47.	26. 41. 71. 44. 60.	14. 65. 32. 51. 25.	20. 42. 91. 18.

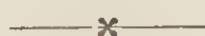
Tafel II (Artikel 99).

	−1.	+2.	+3.	+5.	+7.	+11.	+13.	+17.	+19.	+23.	+29.	+31.	+37.	+41.	+43.	+47.	+53.	+59.	+61.	+67.	+71.	+73.	+79.	+83.	+89.	+97.
3.			—		—		—		—			—	—		—				—	—		—	—			—
5.	—			—		—			—		—	—		—				—	—		—		—		—	
7.		—			—	—				—	—		—		—		—			—	—		—			
11.			—	—		—				—		—	—			—	—	—		—	—				—	—
13.	—		—				—	—		—	—				—		—		—				—			
17.	—	—					—	—	—						—	—	—	—		—				—	—	
19.				—	—	—		—	—	—					—	—			—			—		—		
23.		—	—				—			—	—	—		—		—		—			—	—				
29.	—			—	—		—			—	—						—	—		—	—			—		
31.		—		—	—				—			—		—		—		—		—	—					—
37.	—		—		—	—							—	—		—	—			—	—	—		—		
41.	—	—		—						—		—	—	—	—			—	—			—		—		
43.						—	—	—		—		—		—	—	—	—	—		—			—	—		—
47.		—	—		—			—					—			—	—	—	—		—		—	—	—	—
53.	—				—	—	—	—			—		—		—	—	—	—							—	—
59.			—	—	—			—	—		—			—			—	—			—		—			
61.	—		—	—			—		—					—		—			—			—		—		—
67.								—	—	—	—		—			—		—		—	—	—		—	—	
71.		—	—	—					—		—		—		—						—	—	—	—	—	
73.	—	—	—						—	—			—	—					—	—	—	—	—		—	—
79.		—		—		—	—		—	—		—								—		—	—	—	—	—
83.			—		—	—		—		—	—	—	—	—				—	—					—		
89.	—	—		—		—		—								—	—			—	—	—	—		—	—
97.	—	—	—			—						—			—	—	—		—			—	—		—	—

Tafel III (Artikel 316).

3.	(0)..3; (1)..6.
7.	(0)..142857.
9.	(0)..1; (1)..2; (2)..4; (3)..8; (4)..7; (5)..5.
11.	(0)..09; (1)..18; (2)..36; (3)..72; (4)..45.
13.	(0)..076923; (1)..461538.
17.	(0)..0588235294 117647.
19.	(0)..0526315789 47368421.
23.	(0)..0434782608 6956521739 13.
27.	(0)..037; (1)..074; (2)..148; (3)..296; (4)..592; (5)..185.
29.	(0)..0344827586 2068965517 24137931.
31.	(0)..032280645 16129; (1)..5483870967 74193.
37.	(0)..027; (1)..135; (2)..675; (3)..378; (4)..891; (5)..459;
	(6)..297; (7)..486; (8)..432; (9)..162; (10)..810; (11)..054.
41.	(0)..02439; (1)..14634; (2)..87804; (3)..26829;
	(4)..60975; (5)..65853; (6)..95121; (7)..70731.
43.	(0)..0232558139 5348837209 3; (1)..6511627906 9767441860 4.
47.	(0)..0212765957 4468085106 3829787234 0425531914 893617.
49.	(0)..0204081632 6530612244 8979591836 7346938775 51.
53.	(0)..0188679245 283; (1)..4905660377 358;
	(2)..7547169811 320; (3)..6226415094 339.
59.	(0)..0169491525 4237288135 5932203389 8305084745 7627118644
	06779661.
61.	(0)..0163934426 2295081967 2131147540 9836065573 7704918032
	7868852459.
67.	(0)..0149253731 3432835820 8955223880 597;
	(1)..1791044776 1194029850 7462686567 164.
71.	(0)..0140845070 4225352112 6760563380 28169;
	(1)..8732394366 1971830985 9154929577 46478.
73.	(0)..01369863; (1)..06849315; (2)..34246575;
	(3)..71232876; (4)..56164383; (5)..80821917;
	(6)..04109589; (7)..20547945; (8)..02739726.
79.	(0)..0126582278 481; (1)..3670886075 949; (2)..6455696202 531;
	(3)..7215189873 417; (4)..9240506329 113; (5)..7974683544 303.
81.	(0)..012345679; (1)..135802469; (2)..493827160;
	(3)..432098765; (4)..753086419; (5)..283950617.
83.	(0)..0120481927 7108433734 9397590361 4457831325 3;
	(1)..6024096385 5421686746 9879518072 2891566265 0.
89.	(0)..0112359550 5617977528 0898876404 4943820224 7191;
	(1)..3370786516 8539325842 6966292134 8314606741 5730.
97.	(0)..0103092783 5051546391 7525773195 8762886597 9381443298
	9690721649 4845360824 7422680412 3711340206 185567.

Abhandlungen.



Neuer Beweis eines arithmetischen Satzes.

(Commentationes soc. reg. sc. Gottingensis, Vol. XVI, Gottingae 1808.)

1.

Fragen aus der höheren Arithmetik bieten sehr häufig eine eigentümliche Erscheinung dar, welche in der Analysis weit seltener vorkommt und zur Erhöhung ihrer Reize wesentlich beiträgt. Während man nämlich bei analytischen Untersuchungen meistenteils zu neuen Wahrheiten nur dann gelangen kann, wenn man die Prinzipien, auf denen sie beruhen und die zu ihnen gewissermassen den Weg öffnen sollen, völlig in seiner Gewalt hat, springen einem dagegen in der Arithmetik sehr häufig auf dem Wege der Induction durch einen unerwarteten Zufall die elegantesten Wahrheiten in die Augen, deren Beweise so tief versteckt liegen und in solches Dunkel gehüllt sind, dass sie allen Versuchen spotten und den scharfsinnigsten Forschungen sich nicht zugänglich erweisen. Ferner besteht zwischen arithmetischen Wahrheiten, die auf den ersten Anblick höchst verschiedener Natur sind, ein so enger und so wunderbarer Zusammenhang, dass man nicht selten, während man etwas ganz anderes sucht, endlich zu einem so sehr ersehnten und durch lange Überlegungen vorher vergeblich gesuchten Beweise auf ganz verschiedenem Wege, als man erwartet hatte, gelangt. Meistenteils aber sind solche Wahrheiten von der Art, dass man zu ihnen auf mehreren sehr verschiedenen Wegen kommen kann, und es sind nicht immer die kürzesten Wege, welche sich zuerst darbieten. Man wird es daher sicherlich hoch zu schätzen haben, wenn es einem, nachdem man eine solche Wahrheit lange vergeblich überdacht und sodann zwar bewiesen, aber auf versteckter liegenden Umwegen bewiesen hat, endlich gelingt, den einfachsten und natürlichsten Weg zu entdecken.

2.

Unter den Fragen, von denen wir im vorigen Artikel gesprochen haben, nimmt das beinahe die ganze Theorie der quadratischen Reste enthaltende Theorem, welches wir in den „*Arithmetischen Untersuchungen*“ (Abschnitt IV) durch den Namen des **Fundamentalsatzes** ausgezeichnet haben, einen hervor-

ragenden Platz ein. Für den ersten Erfinder dieses höchst eleganten Satzes hat man unzweifelhaft Legendre zu halten, nachdem schon lange vorher die grossen Geometer Euler und Lagrange mehrere Specialfälle desselben auf inductivem Wege entdeckt hatten. Mit der Aufzählung der Versuche dieser Männer, den Satz zu beweisen, halte ich mich hier nicht auf; wem es Vergnügen macht, möge das eben erwähnte Werk nachlesen. Es möge mir nur zur Bekräftigung des im vorigen Artikel Gesagten gestattet sein, das auf meine eigenen Versuche Bezügliche hinzuzufügen. Auf den Satz selbst kam ich ganz allein im Jahre 1795, als ich noch mit Allem dem, was in der höheren Arithmetik bis dahin gearbeitet worden war, gänzlich unbekannt und aller litterarischen Hülfsmittel entblösst war; doch quälte mich dasselbe das ganze Jahr hindurch und spottete auch der angestrengtesten Bemühung, bis ich endlich den im vierten Abschnitt jenes Werkes angeführten Beweis erhielt. Nachher boten sich mir drei andere, auf ganz verschiedenen Prinzipien beruhende Beweise dar, von denen ich den einen im fünften Abschnitt mitgeteilt habe, die übrigen aber, welche an Eleganz jenem nicht nachstehen, bei anderer Gelegenheit veröffentlichen werde. Alle diese Beweise aber, die zwar in Bezug auf Strenge nichts zu wünschen übrig lassen dürften, sind aus allzu heterogenen Prinzipien abgeleitet, mit Ausnahme vielleicht des ersten, der jedoch durch eine sehr mühselige Schlussreihe hin fortschreitet und an zu weitläufigen Operationen leidet. Ich trage daher kein Bedenken, es auszusprechen, dass es bisher an einem natürlichen Beweise gefehlt hat; Kundige mögen aber beurteilen, ob der, dessen Entdeckung uns neulich gelungen ist, und den die folgenden Seiten darlegen, mit diesem Namen ausgezeichnet zu werden verdient.

3.

Satz. Es sei p eine positive Primzahl, k eine beliebige durch p nicht teilbare ganze Zahl,

A der Complex der Zahlen $1, 2, 3, \ldots, \frac{1}{2}(p-1)$,

B der Complex der Zahlen $\frac{1}{2}(p+1), \frac{1}{2}(p+3), \frac{1}{2}(p+5), \ldots, p-1$.

Man nehme ferner die kleinsten positiven Reste der Producte aus k und den einzelnen Zahlen A nach dem Modul p, welche offenbar sämtlich verschieden sein und teils zu A teils zu B gehören werden. Nimmt man nun an, dass zu B im Ganzen μ Reste gehören, so wird k quadratischer Rest oder Nichtrest von p sein, je nachdem μ gerade oder ungerade ist.

Beweis. Sind $a, a', a'', \ldots$ die zu A, $b, b', b'', \ldots$ aber die übrigen zu B gehörigen Reste, so werden offenbar die Complemente der letzteren $p-b, p-b', p-b'', \ldots$ sämtlich von den Zahlen $a, a', a'', \ldots$ verschieden sein, aber mit diesen zusammengenommen den ganzen Complex A ausmachen. Man hat daher:

$$1 \cdot 2 \cdot 3 \ldots . \frac{1}{2}(p-1) = aa'a'' \ldots (p-b)(p-b')(p-b'') \ldots$$

Das letztere Product aber wird offenbar:

$$\begin{aligned}&\equiv(-1)^{\mu}aa'a''\cdots bb'b''\cdots\\&\equiv(-1)^{\mu}k\cdot 2k\cdot 3k\cdot\cdots\cdot\tfrac{1}{2}(p-1)k\\&\equiv(-1)^{\mu}k^{\frac{1}{2}(p-1)}\cdot 1\cdot 2\cdot 3\cdot\cdots\cdot\tfrac{1}{2}(p-1)\ (\mathrm{mod.}\ p).\end{aligned}$$

Hiernach ist:

$$1\equiv(-1)^{\mu}k^{\frac{1}{2}(p-1)},$$

oder $k^{\frac{1}{2}(p-1)}\equiv\pm1$, je nachdem μ gerade oder ungerade ist, woraus unser Satz sogleich sich ergiebt.

4.

Die folgenden Schlüsse kann man durch Einführung einiger passender Bezeichnungen bedeutend abkürzen. Es möge also das Zeichen (k, p) die Anzahl derjenigen Producte aus der Reihe

$$k,\ 2k,\ 3k,\ \ldots,\ \tfrac{1}{2}(p-1)k$$

ausdrücken, deren kleinste positive Reste nach dem Modul p die Hälfte desselben übersteigen. Ist ferner x irgend eine nicht ganzzahlige Grösse, so werden wir durch das Zeichen $[x]$ die x am nächsten liegende kleinere ganze Zahl darstellen, so dass $x-[x]$ stets eine positive, zwischen den Grenzen 0 und 1 liegende Grösse ist. Mit geringer Mühe entwickelt man dann die folgenden Beziehungen:

I. $[x]+[-x]=-1$.

II. $[x]+h=[x+h]$, so oft h eine ganze Zahl ist.

III. $[x]+[h-x]=h-1$.

IV. Ist $x-[x]$ ein Bruch kleiner als $\frac{1}{2}$, so ist $[2x]-2[x]=0$; ist dagegen $x-[x]>\frac{1}{2}$, so ist $[2x]-2[x]=1$.

V. Liegt daher der kleinste positive Rest der ganzen Zahl h nach dem Modul p unterhalb $\frac{1}{2}p$, so ist $\left[\frac{2h}{p}\right]-2\left[\frac{h}{p}\right]=0$; liegt aber jener Rest oberhalb $\frac{1}{2}p$, so ist $\left[\frac{2h}{p}\right]-2\left[\frac{h}{p}\right]=1$.

VI. Hieraus folgt sogleich:

$$\begin{aligned}(k, p)=&\left[\frac{2k}{p}\right]+\left[\frac{4k}{p}\right]+\left[\frac{8k}{p}\right]+\cdots+\left[\frac{(p-1)k}{p}\right]\\&-2\left[\frac{k}{p}\right]-2\left[\frac{2k}{p}\right]-2\left[\frac{3k}{p}\right]-\cdots-2\left[\frac{\frac{1}{2}(p-1)k}{p}\right].\end{aligned}$$

VII. Aus VI. und I. leitet man ohne Mühe her:

$$(k, p)+(-k, p)=\tfrac{1}{2}(p-1).$$

Hieraus ergiebt sich, dass $-k$ entweder dieselbe oder die entgegengesetzte Beziehung zu p hat (insofern es nämlich quadratischer Rest oder Nichtrest von p ist) wie $+k$, je nachdem p entweder von der Form $4n+1$

oder von der Form $4n+3$ ist. Im ersten Falle ist offenbar -1 Rest, im zweiten Nichtrest von p.

VIII. Die in VI. angegebene Formel ändern wir in folgender Weise um. Nach III. wird:

$$\left[\frac{(p-1)k}{p}\right] = k-1-\left[\frac{k}{p}\right],\quad \left[\frac{(p-3)k}{p}\right] = k-1-\left[\frac{3k}{p}\right],$$
$$\left[\frac{(p-5)k}{p}\right] = k-1-\left[\frac{5k}{p}\right], \ldots .$$

Wenden wir diese Substitutionen auf die $\frac{p\mp 1}{4}$ letzten Glieder der oberen Reihe in jenem Ausdruck an, so erhalten wir:
erstens, so oft p von der Form $4n+1$ ist:

$$\begin{aligned}(k, p) = \tfrac{1}{4}(k-1)(p-1) & \\ -2\left\{\left[\frac{k}{p}\right]+\left[\frac{3k}{p}\right]+\left[\frac{5k}{p}\right]+\cdots+\left[\frac{\frac{1}{2}(p-3)k}{p}\right]\right\} & \\ -\left\{\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]+\cdots+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\right\}; &\end{aligned}$$

zweitens, so oft p von der Form $4n+3$ ist:

$$\begin{aligned}(k, p) = \tfrac{1}{4}(k-1)(p+1) & \\ -2\left\{\left[\frac{k}{p}\right]+\left[\frac{3k}{p}\right]+\left[\frac{5k}{p}\right]+\cdots+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\right\} & \\ -\left\{\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]+\cdots+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\right\}. &\end{aligned}$$

IX. Für den speciellen Fall $k=+2$ ergiebt sich aus den eben angegebenen Formeln: $(2, p) = \frac{1}{4}(p\mp 1)$, wo das obere oder untere Zeichen zu nehmen ist, je nachdem p von der Form $4n+1$ oder $4n+3$ ist. Es wird daher $(2, p)$ gerade und daher 2 Rest von p, so oft p von der Form $8n+1$ oder $8n+7$ ist; dagegen wird $(2, p)$ ungerade und daher 2 Nichtrest von p, so oft p von der Form $8n+3$ oder $8n+5$ ist.

5.

Satz. Es sei x eine positive nicht ganzzahlige Grösse von der Art, dass unter ihren Vielfachen $x, 2x, 3x, \ldots$ bis zu nx keins eine ganze Zahl wird, und man setze $[nx]=h$, woraus leicht folgt, dass sich auch unter den Vielfachen der reciproken Grösse $\frac{1}{x}, \frac{2}{x}, \frac{3}{x}, \ldots$ bis zu $\frac{h}{x}$ keine ganze Zahl vorfindet. Dann behaupte ich, dass

$$\left.\begin{aligned}[x] + [2x] + [3x] + \cdots + [nx] \\ +\left[\frac{1}{x}\right]+\left[\frac{2}{x}\right]+\left[\frac{3}{x}\right]+\cdots+\left[\frac{h}{x}\right]\end{aligned}\right\} = nh$$

ist.

Beweis. Die ersten Glieder der Reihe $[x]+[2x]+[3x]+\cdots+[nx]$, welche wir gleich Ω setzen wollen, bis zum $\left[\frac{1}{x}\right]$ten einschliesslich sind offenbar sämtlich gleich 0, die folgenden bis zum $\left[\frac{2}{x}\right]$ten sämtlich gleich 1, die folgenden bis zum $\left[\frac{3}{x}\right]$ten sämtlich gleich 2 u. s. w. Daher wird:

$$\left.\begin{aligned}\Omega = 0\cdot &\left[\frac{1}{x}\right]\\ +1\cdot &\left\{\left[\frac{2}{x}\right]-\left[\frac{1}{x}\right]\right\}\\ +2\cdot &\left\{\left[\frac{3}{x}\right]-\left[\frac{2}{x}\right]\right\}\\ +3\cdot &\left\{\left[\frac{4}{x}\right]-\left[\frac{3}{x}\right]\right\}\\ +\cdots&\cdots\cdots\\ +(h-1)\cdot &\left\{\left[\frac{h}{x}\right]-\left[\frac{h-1}{x}\right]\right\}\\ +\quad h\quad\cdot &\left\{n-\left[\frac{h}{x}\right]\right\}\end{aligned}\right\} = hn-\left[\frac{1}{x}\right]-\left[\frac{2}{x}\right]-\left[\frac{3}{x}\right]-\cdots-\left[\frac{h}{x}\right].$$

W. z. b. w.

6.

Satz. Bezeichnen k, p beliebige positive ungleiche zu einander prime Zahlen, so ist:

$$\left.\begin{aligned}&\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]+\cdots+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\\ +&\left[\frac{p}{k}\right]+\left[\frac{2p}{k}\right]+\left[\frac{3p}{k}\right]+\cdots+\left[\frac{\frac{1}{2}(k-1)p}{k}\right]\end{aligned}\right\} = \tfrac{1}{4}(k-1)(p-1).$$

Beweis. Nimmt man, was erlaubt ist, an, dass $k<p$ ist, so wird $\frac{\frac{1}{2}(p-1)k}{p}$ kleiner als $\frac{1}{2}k$, aber grösser als $\frac{1}{2}(k-1)$ und daher $\left[\frac{\frac{1}{2}(p-1)k}{p}\right] = \frac{1}{2}(k-1)$ sein. Hieraus geht hervor, dass der vorliegende Satz aus dem vorhergehenden sogleich sich ergiebt, wenn man daselbst $\frac{k}{p}=x$, $\frac{1}{2}(p-1)=n$ und daher $\frac{1}{2}(k-1)=h$ setzt.

Ferner kann man in ähnlicher Weise zeigen, dass, wenn k eine gerade zu p prime Zahl ist,

$$\left.\begin{aligned}&\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]+\cdots+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\\ +&\left[\frac{p}{k}\right]+\left[\frac{2p}{k}\right]+\left[\frac{3p}{k}\right]+\cdots+\left[\frac{\frac{1}{2}kp}{k}\right]\end{aligned}\right\} = \tfrac{1}{4}k(p-1)$$

sein wird. Doch halten wir uns mit diesem für unsern Zweck nicht erforderlichen Satze nicht auf.

7.

Nunmehr ergiebt sich aus der Verbindung des vorigen Satzes mit dem Satze VIII des Artikels 4 sogleich das Fundamentaltheorem. Bezeichnen nämlich k, p irgend welche ungleichen positiven Primzahlen, und setzt man:

$$(k,p)+\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]+\cdots+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]=L$$
$$(p,k)+\left[\frac{p}{k}\right]+\left[\frac{2p}{k}\right]+\left[\frac{3p}{k}\right]+\cdots+\left[\frac{\frac{1}{2}(k-1)p}{k}\right]=M,$$

so geht aus VIII. im Artikel 4 hervor, dass L und M immer gerade Zahlen werden. Nach dem Satze des Artikels 6 aber ist:

$$L+M=(k,p)+(p,k)+\tfrac{1}{4}(k-1)(p-1).$$

So oft daher $\frac{1}{4}(k-1)(p-1)$ gerade wird, was geschieht, wenn entweder jede der beiden Zahlen k, p oder wenigstens eine von der Form $4n+1$ ist, so müssen notwendig (k, p) und (p, k) entweder beide gerade oder beide ungerade sein. So oft aber $\frac{1}{4}(k-1)(p-1)$ ungerade ist, was der Fall ist, wenn jede der beiden Zahlen k, p von der Form $4n+3$ ist, so muss notwendig die eine der beiden Zahlen (k, p), (p, k) gerade, die andere ungerade sein. Im ersten Falle ist daher die Beziehung von k zu p mit der Beziehung von p zu k (insofern nämlich die eine Rest oder Nichtrest der andern ist) identisch, im zweiten Falle aber derselben entgegengesetzt. W. z. b. w.

Summierung gewisser Reihen von besonderer Art.

(Commentationes soc. reg. sc. Gotting. recentiores, Vol. I, Gottingae 1811.)

1.

Unter den ausgezeichneteren Wahrheiten, zu denen die Lehre von der Teilung des Kreises den Weg geöffnet hat, nimmt die im Artikel 356 der „*Arithmetischen Untersuchungen*" angegebene Summation nicht den letzten Platz ein, nicht nur wegen ihrer besonderen Eleganz und wunderbaren Fruchtbarkeit, die ausführlicher darzulegen uns nacher eine andere Untersuchung Gelegenheit geben wird, sondern auch aus dem Grunde, weil ein strenger und vollständiger Beweis derselben nicht gewöhnlichen Schwierigkeiten begegnet. Diese hätten gewiss um so weniger erwartet werden dürfen, als sie nicht sowohl den Satz selbst als vielmehr eine gewisse Bestimmung des Satzes betreffen, bei deren Nichtberücksichtigung der Beweis sogleich auf der Hand liegt und sehr leicht aus der in jenem Werke entwickelten Theorie sich ergiebt. Das Theorem ist dort in folgender Form dargestellt worden. Nimmt man an, dass n eine Primzahl sei, und bezeichnet man unbestimmt alle zwischen den Grenzen 0 und $n-1$ incl. gelegenen quadratischen Reste von n mit a und alle zwischen denselben Grenzen liegenden Nichtreste mit b, endlich mit ω den Bogen $\frac{360^\circ}{n}$ und mit k irgend eine durch n nicht teilbare gegebene ganze Zahl, so ist:

I. Für einen Wert von n, der von der Form $4m+1$ ist:

$$\Sigma \cos ak\omega = -\tfrac{1}{2} \pm \tfrac{1}{2}\sqrt{n}$$

$$\Sigma \cos bk\omega = -\tfrac{1}{2} \mp \tfrac{1}{2}\sqrt{n}, \text{ und daher:}$$

$$\Sigma \cos ak\omega - \Sigma \cos bk\omega = \pm\sqrt{n}$$

$$\Sigma \sin ak\omega = 0$$

$$\Sigma \sin bk\omega = 0.$$

II. Für einen Wert von n, der von der Form $4m+3$ ist:

$$\begin{aligned} \Sigma \cos ak\omega &= -\tfrac{1}{2}\\ \Sigma \cos bk\omega &= -\tfrac{1}{2}\\ \Sigma \sin ak\omega &= \pm \tfrac{1}{2}\sqrt{n}\\ \Sigma \sin bk\omega &= \mp \tfrac{1}{2}\sqrt{n}\\ \Sigma \sin ak\omega - \Sigma \sin bk\omega &= \pm \sqrt{n}. \end{aligned}$$

Die Summationen sind am erwähnten Orte mit aller Strenge bewiesen worden und es bleibt hier keine andere Schwierigkeit weiter übrig als die Bestimmung des der Wurzelgrösse beizulegenden **Vorzeichens.** Es lässt sich zwar ohne Mühe zeigen, dass dieses Vorzeichen von der Zahl k insoweit abhängt, als stets für sämtliche Werte von k, welche quadratische Reste von n sind, dasselbe Zeichen, für alle Werte aber von k, welche quadratische Nichtreste von n sind, das jenem entgegengesetzte Vorzeichen gelten muss. Daher dreht sich die ganze Sache um den Wert $k=1$, und es ist klar, dass, sobald man einmal das für diesen Wert geltende Vorzeichen kennt, auch für alle übrigen Werte von k die Vorzeichen sogleich bekannt sind. Aber gerade bei dieser Untersuchung, welche auf den ersten Anblick zu den leichteren zu gehören scheint, treffen wir auf ganz unerwartete Schwierigkeiten, und das Verfahren, durch dessen Führung wir soweit ohne Hindernisse gekommen waren, versagt ganz und gar die weitere Hülfe.

2.

Es wird nicht unzweckmässig sein, wenn wir, bevor wir weiter gehen, einige **Beispiele** unsrer Summation mittelst numerischer Berechnung entwickeln; doch wird es gut sein, dieser einige allgemeine Bemerkungen vorauszuschicken.

I. Wenn in dem Falle, wo n eine Primzahl von der Form $4m+1$ ist, sämtliche quadratischen Reste von n zwischen den Grenzen 1 und $\frac{1}{2}(n-1)$ einschliesslich unbestimmt durch a' und alle Nichtreste zwischen denselben Grenzen durch b' dargestellt werden, so sind bekanntlich sämtliche $n-a'$ unter den a und sämtliche $n-b'$ unter den b enthalten; mithin werden, da sämtliche a', b', $n-a'$, $n-b'$ offenbar den ganzen Complex der Zahlen 1, 2, 3, ..., $n-1$ ausmachen, sämtliche a' zusammen mit sämtlichen $n-a'$ sämtliche a umfassen und ebenso sämtliche b' zusammen mit sämtlichen $n-b'$ sämtliche b darstellen. Hiernach ist:

$$\begin{aligned} \Sigma \cos ak\omega &= \Sigma \cos a'k\omega + \Sigma \cos(n-a')k\omega\\ \Sigma \cos bk\omega &= \Sigma \cos b'k\omega + \Sigma \cos(n-b')k\omega\\ \Sigma \sin ak\omega &= \Sigma \sin a'k\omega + \Sigma \sin(n-a')k\omega\\ \Sigma \sin bk\omega &= \Sigma \sin b'k\omega + \Sigma \sin(n-b')k\omega. \end{aligned}$$

Da man nun $\cos(n-a')k\omega = \cos a'k\omega$, $\cos(n-b')k\omega = \cos b'k\omega$, $\sin(n-a')k\omega = -\sin a'k\omega$, $\sin(n-b')k\omega = -\sin b'k\omega$ hat, so wird offenbar ohne Weiteres:

$$\Sigma \sin ak\omega = \Sigma \sin a'k\omega - \Sigma \sin a'k\omega = 0$$
$$\Sigma \sin bk\omega = \Sigma \sin b'k\omega - \Sigma \sin b'k\omega = 0.$$

Die Summe der Cosinus aber nimmt die Form an:

$$\Sigma \cos ak\omega = 2\Sigma \cos a'k\omega$$
$$\Sigma \cos bk\omega = 2\Sigma \cos b'k\omega,$$

so dass also werden muss:

$$1 + 4\Sigma \cos a'k\omega = \pm \sqrt{n}$$
$$1 + 4\Sigma \cos b'k\omega = \mp \sqrt{n}$$
$$2\Sigma \cos a'k\omega - 2\Sigma \cos b'k\omega = \pm \sqrt{n}.$$

II. In dem Falle, wo n von der Form $4m+3$ ist, ist das Complement eines jeden Restes a zu n Nichtrest und das Complement eines jeden b Rest; daher werden sämtliche $n-a$ mit sämtlichen b und sämtliche $n-b$ mit sämtlichen a übereinstimmen. Hieraus folgt:

$$\Sigma \cos ak\omega = \Sigma \cos(n-b)k\omega = \Sigma \cos bk\omega.$$

Somit sind, da sämtliche a und b zusammen sämtliche Zahlen $1, 2, 3, \ldots n-1$ ausmachen und daher $\Sigma \cos ak\omega + \Sigma \cos bk\omega = \cos k\omega + \cos 2k\omega + \cos 3k\omega + \cdots + \cos(n-1)k\omega = -1$ wird, die Summationen

$$\Sigma \cos ak\omega = -\tfrac{1}{2}$$
$$\Sigma \cos bk\omega = -\tfrac{1}{2}$$

ohne weiteres klar. Ebenso ist:

$$\Sigma \sin ak\omega = \Sigma \sin(n-b)k\omega = -\Sigma \sin bk\omega,$$

woraus hervorgeht, in welcher Weise die eine der beiden Summationen

$$2\Sigma \sin ak\omega = \pm \sqrt{n}$$
$$2\Sigma \sin bk\omega = \mp \sqrt{n}$$

von der andern abhängig ist.

3.

Im Nachstehenden sieht man nun die numerische Berechnung für einige Beispiele.

I. Für $n=5$ giebt es einen Wert von a', nämlich $a'=1$, und einen Wert von b', nämlich $b'=2$. Nun ist aber:

$$\cos\omega = +0{,}3090169944 \qquad \cos 2\omega = -0{,}8090169944;$$

mithin: $1 + 4\cos\omega = +\sqrt{5}$, $1 + 4\cos 2\omega = -\sqrt{5}$.

II. Für $n = 13$ giebt es drei Werte von a', nämlich 1, 3, 4, und ebenso viele Werte von b', nämlich 2, 5, 6, wonach wir berechnen:

$$\begin{array}{rlrl} \cos\omega &= +0{,}8854560257 & \cos 2\omega &= +0{,}5680647467 \\ \cos 3\omega &= +0{,}1205366803 & \cos 5\omega &= -0{,}7485107482 \\ \cos 4\omega &= -0{,}3546048870 & \cos 6\omega &= -0{,}9709418174 \\ \hline \text{Summe} &= +0{,}6513878190 & \text{Summe} &= -1{,}1513878189 \end{array}$$

Daher: $1 + 4\Sigma\cos a'\omega = +\sqrt{13}$, $1 + 4\Sigma\cos b'\omega = -\sqrt{13}$.

III. Für $n = 17$ haben wir vier Werte von a', nämlich 1, 2, 4, 8, und ebenso viele Werte von b', nämlich 3, 5, 6, 7. Hiernach berechnen sich die Cosinus:

$$\begin{array}{rlrl} \cos\omega &= +0{,}9324722294 & \cos 3\omega &= +0{,}4457383558 \\ \cos 2\omega &= +0{,}7390089172 & \cos 5\omega &= -0{,}2736629901 \\ \cos 4\omega &= +0{,}0922683595 & \cos 6\omega &= -0{,}6026346364 \\ \cos 8\omega &= -0{,}9829730997 & \cos 7\omega &= -0{,}8502171357 \\ \hline \text{Summe} &= +0{,}7807764064 & \text{Summe} &= -1{,}2807764065 \end{array}$$

Daher $1 + 4\Sigma\cos a'\omega = +\sqrt{17}$, $1 + 4\Sigma\cos b'\omega = -\sqrt{17}$.

IV. Für $n = 3$ giebt es nur einen Wert von a, nämlich $a = 1$, und diesem entspricht

$$\sin\omega = +0{,}8660254038.$$

Daher: $2\sin\omega = +\sqrt{3}$.

V. Für $n = 7$ giebt es drei Werte von a, nämlich 1, 2, 4; demnach hat man die Sinus:

$$\begin{array}{rl} \sin\omega &= +0{,}7818314825 \\ \sin 2\omega &= +0{,}9749279122 \\ \sin 4\omega &= -0{,}4338837391 \\ \hline \text{Summe} &= +1{,}3228756556, \end{array}$$

und daher: $2\Sigma\sin a\omega = +\sqrt{7}$.

VI. Für $n = 11$ sind die Werte von a: 1, 3, 4, 5, 9, und diesen entsprechen die Sinus:

$$\begin{array}{rl} \sin\omega &= +0{,}5406408175 \\ \sin 3\omega &= +0{,}9898214419 \\ \sin 4\omega &= +0{,}7557495744 \\ \sin 5\omega &= +0{,}2817325568 \\ \sin 9\omega &= -0{,}9096319954 \\ \hline \text{Summe} &= +1{,}6583123952, \end{array}$$

und daher: $2\Sigma\sin a\omega = +\sqrt{11}$.

VII. Für $n = 19$ sind die Werte von a: 1, 4, 5, 6, 7, 9, 11, 16, 17, und diesen entsprechen die Sinus:

$$\begin{aligned}
\sin \omega &= +0{,}3246994692 \\
\sin 4\omega &= +0{,}9694002659 \\
\sin 5\omega &= +0{,}9965844930 \\
\sin 6\omega &= +0{,}9157733267 \\
\sin 7\omega &= +0{,}7357239107 \\
\sin 9\omega &= +0{,}1645945903 \\
\sin 11\omega &= -0{,}4759473930 \\
\sin 16\omega &= -0{,}8371664783 \\
\sin 17\omega &= -0{,}6142127127 \\
\hline
\text{Summe} &= +2{,}1794494718, \text{ und daher: } 2\Sigma \sin a\omega = +\sqrt{19}.
\end{aligned}$$

4.

In allen diesen Beispielen erhält die Wurzelgrösse das positive Vorzeichen, und eben dieselbe Thatsache bestätigt man leicht für grössere Werte $n = 23$, $n = 29$, u. s. w., woraus sich schon eine hohe Wahrscheinlichkeit dafür ergiebt, dass dies allgemein so sein werde. Aber der Beweis dieser Erscheinung lässt sich nicht aus den am angegebenen Orte auseinandergesetzten Prinzipien ableiten und muss mit vollstem Rechte als viel tiefer liegend erachtet werden. Daher geht das Ziel dieser Abhandlung dahin, einen strengen Beweis dieses höchst eleganten Satzes, den wir einst mehrere Jahre hindurch auf verschiedene Arten vergeblich versucht und schliesslich durch eigentümliche und ziemlich subtile Betrachtungen glücklich zu Stande gebracht haben, anzugeben und zugleich den Satz unbeschadet seiner Eleganz oder vielmehr unter Erhöhung derselben zu weit grösserer Allgemeinheit zu erheben. Am Ende derselben werden wir dann schliesslich den wunderbaren engen Zusammenhang zwischen dieser Summation und einem andern äusserst wichtigen arithmetischen Satze darlegen. Wir hoffen, dass diese Untersuchungen nicht nur an und für sich den Geometern willkommen sein, sondern auch, dass die Methoden, durch welche wir dies alles zu erreichen vermochten und die auch bei andern Gelegenheiten nützlich sein können, ihrer Beachtung wert erscheinen werden.

5.

Unser Beweis gründet sich auf die Betrachtung einer eigentümlichen Art von Reihen, deren Glieder von Ausdrücken wie

$$\frac{(1-x^m)(1-x^{m-1})(1-x^{m-2})\cdots(1-x^{m-\mu+1})}{(1-x)\;(1-x^2)\;(1-x^3)\;\cdots(1-x^\mu)}$$

30*

abhängen. Der Kürze wegen werden wir einen solchen Bruch mit (m, μ) bezeichnen und zunächst einige allgemeine Bemerkungen über derartige Functionen vorausschicken.

I. So oft m eine ganze positive Zahl kleiner als μ ist, verschwindet offenbar die Function (m, μ), da der Zähler den Factor $1 - x^0$ enthält. Für $m = \mu$ werden die Factoren im Zähler in umgekehrter Reihenfolge mit den Factoren im Nenner identisch sein, so dass $(\mu, \mu) = 1$ ist; schliesslich hat man in dem Falle, wo m eine ganze positive Zahl grösser als μ ist, die Formeln:

$$(\mu + 1, \mu) = \frac{1 - x^{\mu+1}}{1 - x} = (\mu + 1, 1)$$

$$(\mu + 2, \mu) = \frac{(1 - x^{\mu+2})(1 - x^{\mu+1})}{(1 - x)(1 - x^2)} = (\mu + 2, 2)$$

$$(\mu + 3, \mu) = \frac{(1 - x^{\mu+3})(1 - x^{\mu+2})(1 - x^{\mu+1})}{(1 - x)(1 - x^2)(1 - x^3)} = (\mu + 3, 3)$$

u. s. w.

und allgemein:

$$(m, \mu) = (m, m - \mu).$$

II. Ferner bestätigt man leicht, dass man allgemein hat:

$$(m, \mu + 1) = (m - 1, \mu + 1) + x^{m-\mu-1}(m - 1, \mu).$$

Da nun ebenso

$$(m - 1, \mu + 1) = (m - 2, \mu + 1) + x^{m-\mu-2}(m - 2, \mu)$$
$$(m - 2, \mu + 1) = (m - 3, \mu + 1) + x^{m-\mu-3}(m - 3, \mu)$$
$$(m - 3, \mu + 1) = (m - 4, \mu + 1) + x^{m-\mu-4}(m - 4, \mu)$$

u. s. w.

ist und diese Reihe fortgesetzt werden kann bis zu

$$\begin{aligned}(\mu + 2, \mu + 1) &= (\mu + 1, \mu + 1) + x(\mu + 1, \mu)\\ &= (\mu, \mu) + x(\mu + 1, \mu),\end{aligned}$$

wofern nämlich m eine ganze positive Zahl grösser als $\mu + 1$ ist, so wird:

$$(m, \mu + 1) = (\mu, \mu) + x(\mu + 1, \mu) + x^2(\mu + 2, \mu) + x^3(\mu + 3, \mu) + \cdots + x^{m-\mu-1}(m - 1, \mu).$$

Hieraus geht hervor, dass, wenn für irgend einen bestimmten Wert von μ jede Function (m, μ), wo m eine ganze positive Zahl darstellt, eine

ganze Function ist, auch jede Function $(m, \mu+1)$ eine ganze Function werden muss. Da nun jene Annahme für $\mu = 1$ stattfindet, so wird dieselbe auch für $\mu = 2$ und somit auch für $\mu = 3$ u. s. w. gelten, d. h. es ist allgemein für jeden beliebigen positiven ganzzahligen Wert von m die Function (m, μ) eine ganze Function, oder das Product

$$(1-x^m)(1-x^{m-1})(1-x^{m-2})\ldots(1-x^{m-\mu+1})$$

teilbar durch

$$(1-x)(1-x^2)(1-x^3)\ldots(1-x^\mu).$$

6.

Wir werden nun zwei Reihen betrachten, welche beide zu unserem Ziele führen können. Die erste Reihe ist folgende:

$$1-\frac{1-x^m}{1-x}+\frac{(1-x^m)(1-x^{m-1})}{(1-x)(1-x^2)}-\frac{(1-x^m)(1-x^{m-1})(1-x^{m-2})}{(1-x)(1-x^2)(1-x^3)}+\cdots,$$

oder:

$$1-(m,1)+(m,2)-(m,3)+(m,4)-\cdots,$$

die wir der Kürze wegen mit $f(x, m)$ bezeichnen wollen. Zunächst ist unmittelbar klar, dass diese Reihe, so oft m eine ganze positive Zahl ist, nach dem $(m+1)$ten Gliede (welches gleich ± 1 wird) abbricht, und dass somit in diesem Falle die Summe eine endliche ganze Function von x werden muss. Ferner geht aus Artikel 5, II hervor, dass man allgemein für jeden beliebigen Wert von m hat:

$$\begin{aligned} 1 &= 1 \\ -(m,1) &= -(m-1,1)-x^{m-1} \\ +(m,2) &= +(m-1,2)+x^{m-2}(m-1,1) \\ -(m,3) &= -(m-1,3)-x^{m-3}(m-1,2) \end{aligned}$$

u. s. w.

und daher:

$$f(x,m) = 1-x^{m-1}-(1-x^{m-2})(m-1,1)+(1-x^{m-3})(m-1,2) \\ -(1-x^{m-4})(m-1,3)+\cdots$$

Es ist aber offenbar:

$$\begin{aligned} (1-x^{m-2})(m-1,1) &= (1-x^{m-1})(m-2,1) \\ (1-x^{m-3})(m-1,2) &= (1-x^{m-1})(m-2,2) \\ (1-x^{m-4})(m-1,3) &= (1-x^{m-1})(m-2,3) \end{aligned}$$

u. s. w.,

demnach erhalten wir die Gleichung:

[1] $$f(x, m) = (1 - x^{m-1}) f(x, m-2).$$

7.

Da für $m = 0$ $f(x, m) = 1$ wird, so ist nach der soeben gefundenen Formel:

$$f(x, 2) = 1 - x$$
$$f(x, 4) = (1 - x)(1 - x^3)$$
$$f(x, 6) = (1 - x)(1 - x^3)(1 - x^5)$$
$$f(x, 8) = (1 - x)(1 - x^3)(1 - x^5)(1 - x^7)$$
u. s. w.,

oder allgemein für jeden geraden Wert von m:

[2] $$f(x, m) = (1 - x)(1 - x^3)(1 - x^5) \ldots . (1 - x^{m-1}).$$

Dagegen wird, da für $m = 1$ $f(x, m) = 0$ ist, auch

$$f(x, 3) = 0$$
$$f(x, 5) = 0$$
$$f(x, 7) = 0$$
u. s. w.,

oder allgemein für jeden ungeraden Wert von m:

$$f(x, m) = 0.$$

Übrigens hätte die letztere Summation schon daraus abgeleitet werden können, dass in der Reihe

$$1 - (m, 1) + (m, 2) - (m, 3) + \cdots + (m, m-1) - (m, m)$$

das letzte Glied sich gegen das erste, das vorletzte gegen das zweite u. s. w. aufhebt.

8.

Für unsern Zweck genügt zwar der Fall, wo m eine ungerade positive ganze Zahl ist; doch wird es wegen der Bedeutung des Gegenstandes nicht reuen, auch über diejenigen Fälle, wo m entweder gebrochen oder negativ ist, einiges hinzugefügt zu haben. Offenbar wird dann unsere Reihe nicht mehr abbrechen, sondern ins Unendliche fortlaufen, und überdies ist leicht ersichtlich, dass dieselbe divergent ist, so oft man x einen Wert kleiner als 1 beilegt, so dass also die Summierung derselben auf Werte von x, welche grösser als 1 sind, beschränkt werden muss.

Der Formel [1] im Artikel 6 zufolge haben wir:

$$f(x, -2) = \frac{1}{1 - \frac{1}{x}}$$

$$f(x, -4) = \frac{1}{1 - \frac{1}{x}} \cdot \frac{1}{1 - \frac{1}{x^3}}$$

$$f(x, -6) = \frac{1}{1 - \frac{1}{x}} \cdot \frac{1}{1 - \frac{1}{x^3}} \cdot \frac{1}{1 - \frac{1}{x^5}}$$

u. s. w.,

so dass also der Wert der Function $f(x, m)$ auch für einen negativen ganzzahligen geraden Wert von x in endlicher Form angebbar ist. Für die übrigen Werte von m aber verwandeln wir die Function $f(x, m)$ auf folgende Weise in ein unendliches Product.

Nimmt m einen unendlich grossen negativen Wert an, so geht die Function $f(x, m)$ über in:

$$1 + \frac{1}{x-1} + \frac{1}{x-1} \cdot \frac{1}{x^2-1} + \frac{1}{x-1} \cdot \frac{1}{x^2-1} \cdot \frac{1}{x^3-1} + \cdots$$

Diese Reihe ist daher gleich dem unendlichen Producte:

$$\frac{1}{1 - \frac{1}{x}} \cdot \frac{1}{1 - \frac{1}{x^3}} \cdot \frac{1}{1 - \frac{1}{x^5}} \cdot \frac{1}{1 - \frac{1}{x^7}} \cdots\cdots$$

Da ferner allgemein

$$f(x, m) = f(x, m - 2\lambda) \cdot (1 - x^{m-1})(1 - x^{m-3})(1 - x^{m-5}) \ldots . (1 - x^{m-2\lambda+1})$$

ist, so wird:

$$f(x, m) = f(x, -\infty) \cdot (1 - x^{m-1})(1 - x^{m-3})(1 - x^{m-5}) \ldots .$$
$$= \frac{1 - x^{m-1}}{1 - x^{-1}} \cdot \frac{1 - x^{m-3}}{1 - x^{-3}} \cdot \frac{1 - x^{m-5}}{1 - x^{-5}} \cdot \frac{1 - x^{m-7}}{1 - x^{-7}} \cdots,$$

und zwar werden diese Factoren offenbar mehr und mehr gegen die Einheit convergieren.

Besondere Beachtung verdient der Fall $m = -1$, in welchem ist:

$$f(x, -1) = 1 + x^{-1} + x^{-3} + x^{-6} + x^{-10} + \cdots.$$

Diese Reihe ist daher gleich dem unendlichen Producte:

$$\frac{1 - x^{-2}}{1 - x^{-1}} \cdot \frac{1 - x^{-4}}{1 - x^{-3}} \cdot \frac{1 - x^{-6}}{1 - x^{-5}} \cdots,$$

oder es ist, wenn man x für x^{-1} schreibt:

$$1 + x + x^3 + x^6 + \cdots = \frac{1-x^2}{1-x} \cdot \frac{1-x^4}{1-x^3} \cdot \frac{1-x^6}{1-x^5} \cdot \frac{1-x^8}{1-x^7} \cdots$$

Diese Gleichheit zwischen zwei ziemlich verwickelten Ausdrücken, auf die wir bei anderer Gelegenheit zurückkommen werden, ist gewiss höchst bemerkenswert.

9.

Zweitens betrachten wir die folgende Reihe:

$$1 + x^{\frac{1}{2}} \frac{1-x^m}{1-x} + x \frac{(1-x^m)(1-x^{m-1})}{(1-x)(1-x^2)} + x^{\frac{3}{2}} \frac{(1-x^m)(1-x^{m-1})(1-x^{m-2})}{(1-x)(1-x^2)(1-x^3)} + \cdots$$

oder

$$1 + x^{\frac{1}{2}}(m, 1) + x(m, 2) + x^{\frac{3}{2}}(m, 3) + x^2(m, 4) + \cdots,$$

welche wir mit $F(x, m)$ bezeichnen wollen. Wir beschränken diese Untersuchung auf den Fall, wo m eine ganze positive Zahl ist, so dass auch diese Reihe stets mit dem $(m+1)$ten Gliede, welches gleich $x^{\frac{1}{2}m}(m, m)$ ist, abbricht. Da

$$(m, m) = 1, \quad (m, m-1) = (m, 1), \quad (m, m-2) = (m, 2), \ldots$$

ist, so kann diese Reihe auch so dargestellt werden:

$$F(x, m) = x^{\frac{1}{2}m} + x^{\frac{1}{2}(m-1)}(m, 1) + x^{\frac{1}{2}(m-2)}(m, 2) + x^{\frac{1}{2}(m-3)}(m, 3) + \cdots$$

Hieraus folgt:

$$(1 + x^{\frac{1}{2}m+\frac{1}{2}}) F(x, m) = 1 + x^{\frac{1}{2}}(m, 1) + x(m, 2) + x^{\frac{3}{2}}(m, 3) + \cdots$$
$$+ x^{\frac{1}{2}} \cdot x^m + x \cdot x^{m-1}(m, 1) + x^{\frac{3}{2}} \cdot x^{m-2}(m, 2) + \cdots$$

Da man nun (Artikel 5, II)

$$(m, 1) + x^m = (m+1, 1)$$
$$(m, 2) + x^{m-1}(m, 1) = (m+1, 2)$$
$$(m, 3) + x^{m-2}(m, 2) = (m+1, 3)$$

u. s. w.

hat, so ergiebt sich:

[3] $$(1 + x^{\frac{1}{2}m+\frac{1}{2}}) F(x, m) = F(x, m+1).$$

Es ist aber $F(x, 0) = 1$; daher wird:

$$F(x, 1) = 1 + x^{\frac{1}{2}}$$
$$F(x, 2) = (1 + x^{\frac{1}{2}})(1 + x)$$
$$F(x, 3) = (1 + x^{\frac{1}{2}})(1 + x)(1 + x^{\frac{3}{2}})$$

u. s. w.,

oder allgemein:

[4] $$F(x, m) = (1 + x^{\frac{1}{2}})(1 + x)(1 + x^{\frac{3}{2}}) \ldots (1 + x^{\frac{1}{2}m}).$$

10.

Nachdem wir diese vorbereitenden Untersuchungen vorausgeschickt haben, gehen wir nun näher auf unsere Aufgabe ein. Da für einen Primzahlwert von n die Quadrate $1, 4, 9, \ldots, \left(\frac{1}{2}(n-1)\right)^2$ sämtlich unter einander nach dem Modul n incongruent sind, so müssen offenbar ihre kleinsten Reste nach diesem Modul mit den Zahlen a identisch sein und daher:

$$\Sigma \cos ak\omega = \cos k\omega + \cos 4k\omega + \cos 9k\omega + \cdots + \cos\left(\tfrac{1}{2}(n-1)\right)^2 k\omega$$
$$\Sigma \sin ak\omega = \sin k\omega + \sin 4k\omega + \sin 9k\omega + \cdots + \sin\left(\tfrac{1}{2}(n-1)\right)^2 k\omega.$$

Ebenso ist auch, da dieselben Quadrate $1, 4, 9 \ldots, \left(\frac{1}{2}(n-1)\right)^2$ in umgekehrter Reihenfolge den Quadraten $\left(\frac{1}{2}(n+1)\right)^2$, $\left(\frac{1}{2}(n+3)\right)^2$, $\left(\frac{1}{2}(n+5)\right)^2, \ldots, (n-1)^2$ congruent sind:

$$\Sigma \cos ak\omega = \cos\left(\tfrac{1}{2}(n+1)\right)^2 k\omega + \cos\left(\tfrac{1}{2}(n+3)\right)^2 k\omega + \cdots + \cos(n-1)^2 k\omega$$
$$\Sigma \sin ak\omega = \sin\left(\tfrac{1}{2}(n+1)\right)^2 k\omega + \sin\left(\tfrac{1}{2}(n+3)\right)^2 k\omega + \cdots + \sin(n-1)^2 k\omega$$

Setzt man daher:

$$T = 1 + \cos k\omega + \cos 4k\omega + \cos 9k\omega + \cdots + \cos(n-1)^2 k\omega$$
$$U = \sin k\omega + \sin 4k\omega + \sin 9k\omega + \cdots + \sin(n-1)^2 k\omega,$$

so ist:

$$1 + 2\,\Sigma \cos ak\omega = T$$
$$2\,\Sigma \sin ak\omega = U.$$

Hieraus geht hervor, dass die im Artikel 1 angeführten Summationen von der Summation der Reihen T und U abhängen; daher werden wir, indem wir jene aufgeben, unsere Untersuchung auf diese erstrecken und in solcher Allgemeinheit erledigen, dass sie nicht nur Primzahlwerte von n, sondern auch beliebige zusammengesetzte Werte umfasst. Die Zahl k aber setzen wir als prim zu n voraus, da der Fall, wo k und n einen gemeinschaftlichen Teiler haben, leicht auf diesen zurückgeführt werden kann.

11.

Bezeichnen wir die imaginäre Grösse $\sqrt{-1}$ mit i und setzen wir:

$$\cos k\omega + i \sin k\omega = r,$$

so ist $r^n = 1$ oder r eine Wurzel der Gleichung $x^n - 1 = 0$. Man sieht leicht, dass sämtliche Zahlen $k, 2k, 3k, \ldots, (n-1)k$ durch n nicht teilbar und nach dem Modul n incongruent sind; demnach sind die Potenzen von r:

$$1, r, r^2, r^3, \ldots, r^{n-1}$$

sämtlich von einander verschieden, jede einzelne aber wird der Gleichung $x^n - 1 = 0$ ebenfalls genügen. Daher werden diese Potenzen sämtliche Wurzeln der Gleichung $x^n - 1 = 0$ darstellen.

Diese Schlüsse würden nicht richtig sein, wenn k einen gemeinschaftlichen Teiler mit n hätte. Denn wenn ν ein solcher gemeinschaftlicher Teiler wäre, so würde $k \cdot \frac{n}{\nu}$ durch n teilbar und daher eine niedrigere Potenz als r^n, nämlich $r^{\frac{n}{\nu}}$, der Einheit gleich sein. In diesem Falle werden also die Potenzen von r höchstens $\frac{n}{\nu}$ Wurzeln der Gleichung $x^n - 1 = 0$ darstellen, und zwar werden sie wirklich soviel verschiedene Wurzeln liefern, wenn ν der grösste gemeinschaftliche Teiler der Zahlen k und n ist. In unserem Falle, wo k und n zu einander prim vorausgesetzt werden, kann man r passend eine **eigentliche** Wurzel der Gleichung $x^n - 1 = 0$ nennen; in dem anderen Falle dagegen, wo k und n einen (grössten) gemeinschaftlichen Teiler ν haben, würde r eine **uneigentliche** Wurzel jener Gleichung heissen; offenbar aber würde dann r eine eigentliche Wurtel der Gleichung $x^{\frac{n}{\nu}} - 1 = 0$ sein. Die einfachste uneigentliche Wurzel ist die Einheit, und in dem andern Falle, wo n eine Primzahl ist, giebt es überhaupt keine andern uneigentlichen Wurzeln weiter.

12.

Wenn wir nun setzen:

$$W = 1 + r + r^4 + r^9 + \cdots + r^{(n-1)^2},$$

so wird offenbar $W = T + iU$ und T der reelle Teil von W, während U aus dem imaginären Teile von W nach Unterdrückung des Factors i hervorgeht. Die ganze Aufgabe ist daher auf die Ermittlung der Summe W reduciert; zu dem Zwecke kann entweder die im Artikel 6 betrachtete Reihe oder diejenige, welche wir im Artikel 9 zu summieren gelehrt haben, angewendet werden, jedoch ist die erstere weniger geeignet in dem Falle, wo n eine gerade Zahl ist. Trotzdem hoffen wir, dass es den Lesern angenehm sein wird, wenn wir den Fall, wo n ungerade ist, nach einer doppelten Methode behandeln.

Wir nehmen also zunächst an, dass n eine ungerade Zahl sei, dass r irgend eine eigentliche Wurzel der Gleichung $x^n - 1 = 0$ bezeichne und dass in der Function $f(x, m)$ $x = r$ und $m = n - 1$ gesetzt werde. Dann wird offenbar:

$$\frac{1 - x^m}{1 - x} = \frac{1 - r^{-1}}{1 - r} = - r^{-1}$$

$$\frac{1 - x^{m-1}}{1 - x^2} = \frac{1 - r^{-2}}{1 - r^2} = - r^{-2}$$

$$\frac{1 - x^{m-2}}{1 - x^3} = \frac{1 - r^{-3}}{1 - r^3} = - r^{-3}$$

u. s. w.

bis zu

$$\frac{1-x}{1-x^m} = \frac{1-r^{-m}}{1-r^m} = -r^{-m}.$$

(Es wird nicht überflüssig sein, darauf hinzuweisen, dass diese Gleichungen nur so lange gelten, als r als eigentliche Wurzel vorausgesetzt wird; denn wenn r eine uneigentliche Wurzel wäre, so würden in einigen von jenen Brüchen Zähler und Nenner gleichzeitig verschwinden und daher die Brüche unbestimmt werden.)

Hieraus leiten wir die folgende Gleichung her:

$$\begin{aligned} f(r, n-1) &= 1 + r^{-1} + r^{-3} + r^{-6} + \cdots + r^{-\frac{1}{2}(n-1)n} \\ &= (1-r)(1-r^3)(1-r^5)\cdots\cdots(1-r^{n-2}). \end{aligned}$$

Dieselbe Gleichung wird auch noch gelten, wenn man r^λ für r substituiert, wo λ eine beliebige zu n prime Zahl bezeichnet; denn dann ist auch r^λ eine eigentliche Wurzel der Gleichung $x^n - 1 = 0$. Schreiben wir daher r^{n-2} oder, was dasselbe ist, r^{-2} für r, so wird:

$$1 + r^2 + r^6 + r^{12} + \cdots + r^{(n-1)n} = (1-r^{-2})(1-r^{-6})(1-r^{-10})\cdots(1-r^{-2(n-2)}).$$

Multiplicieren wir beide Seiten dieser Gleichung mit

$$r \cdot r^3 \cdot r^5 \cdots\cdots r^{n-2} = r^{\frac{1}{4}(n-1)^2},$$

so ergiebt sich wegen

$$\begin{aligned} r^{2+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n-3)^2}, & r^{(n-1)n+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n+1)^2} \\ r^{6+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n-5)^2}, & r^{(n-2)(n-1)+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n+3)^2} \\ r^{12+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n-7)^2}, & r^{(n-3)(n-2)+\frac{1}{4}(n-1)^2} &= r^{\frac{1}{4}(n+5)^2} \end{aligned}$$

u. s. w.

die folgende Gleichung:

$$\begin{aligned} & r^{\frac{1}{4}(n-1)^2} + r^{\frac{1}{4}(n-3)^2} + r^{\frac{1}{4}(n-5)^2} + \cdots\cdots + r + 1 \\ & + r^{\frac{1}{4}(n+1)^2} + r^{\frac{1}{4}(n+3)^2} + r^{\frac{1}{4}(n+5)^2} + \cdots\cdots + r^{\frac{1}{4}(2n-2)^2} \\ & = (r-r^{-1})(r^3-r^{-3})(r^5-r^{-5})\cdots\cdots(r^{n-2}-r^{-n+2}), \end{aligned}$$

oder, wenn man die Glieder der linken Seite anders ordnet:

[5] $$1 + r + r^4 + \cdots + r^{(n-1)^2} = (r-r^{-1})(r^3-r^{-3})(r^5-r^{-5})\cdots(r^{n-2}-r^{-n+2}).$$

13.

Die Factoren der rechten Seite der Gleichung [5] können auch so dargestellt werden:

$$\begin{aligned} r - r^{-1} &= -(r^{n-1} - r^{-n+1}) \\ r^3 - r^{-3} &= -(r^{n-3} - r^{-n+3}) \\ r^5 - r^{-5} &= -(r^{n-5} - r^{-n+5}) \end{aligned}$$

bis zu

$$r^{n-2} - r^{-n+2} = -(r^2 - r^{-2}),$$

wonach die obige Gleichung die folgende Form annimmt:

$$W = (-1)^{\frac{1}{2}(n-1)}(r^2 - r^{-2})(r^4 - r^{-4})(r^6 - r^{-6}) \cdots (r^{n-1} - r^{-n+1}).$$

Multipliciert man diese Gleichung mit [5] in ihrer ursprünglichen Form, so ergiebt sich:

$$W^2 = (-1)^{\frac{1}{2}(n-1)}(r - r^{-1})(r^2 - r^{-2})(r^3 - r^{-3}) \cdots (r^{n-1} - r^{-n+1}),$$

wo $(-1)^{\frac{1}{2}(n-1)}$ entweder gleich $+1$ oder gleich -1 ist, je nachdem n von der Form $4\mu + 1$ oder von der Form $4\mu + 3$ ist. Hieraus folgt:

$$W^2 = \pm r^{\frac{1}{2}(n-1)n}(1 - r^{-2})(1 - r^{-4})(1 - r^{-6}) \cdots (1 - r^{-2(n-1)}).$$

Man sieht aber leicht, dass $r^{-2}, r^{-4}, r^{-6}, \ldots, r^{-2n+2}$ sämtliche Wurzeln der Gleichung $x^n - 1 = 0$ mit Ausnahme von $x = 1$ darstellen, so dass für jeden Wert von x die identische Gleichung stattfinden muss:

$$(x - r^{-2})(x - r^{-4})(x - r^{-6}) \cdots (x - r^{-2n+2}) = x^{n-1} + x^{n-2} + x^{n-3} + \cdots + x + 1.$$

Setzt man daher $x = 1$, so folgt:

$$(1 - r^{-2})(1 - r^{-4})(1 - r^{-6}) \cdots (1 - r^{-2n+2}) = n,$$

und da offenbar $r^{\frac{1}{2}n(n-1)} = 1$ ist, so geht unsere Gleichung in die folgende über:

[6] $$W^2 = \pm n.$$

In dem Falle also, wo n von der Form $4\mu + 1$ ist, wird:

$$W = \pm \sqrt{n} \text{ und somit } T = \pm \sqrt{n}, \; U = 0;$$

in dem andern Falle dagegen, wo n von der Form $4\mu + 3$ ist, wird:

$$W = \pm i\sqrt{n} \text{ und somit } T = 0, \; U = \pm \sqrt{n}.$$

14.

Die Methode des vorhergehenden Artikels bestimmt nur den absoluten Wert der Aggregate T, U und lässt es ungewiss, ob man T im ersteren Falle und U im letzteren gleich $+\sqrt{n}$ oder gleich $-\sqrt{n}$ setzen muss. Dies kann man aber wenigstens für den Fall, wo $k = 1$ ist, aus der Gleichung [5] in folgender Weise entscheiden. Da für $k = 1$

$$r - r^{-1} = 2i \sin \omega$$
$$r^3 - r^{-3} = 2i \sin 3\omega$$
$$r^5 - r^{-5} = 2i \sin 5\omega$$

u. s. w.

ist, so verwandelt sich jene Gleichung in

$$W = (2i)^{\frac{1}{2}(n-1)} \sin\omega \sin 3\omega \sin 5\omega \ldots \sin(n-2)\omega.$$

Nun kommen in dem Falle, wo n von der Form $4\mu + 1$ ist, in der Reihe der ungeraden Zahlen

$$1, 3, 5, 7, \ldots, \tfrac{1}{2}(n-3), \tfrac{1}{2}(n+1), \ldots, n-2$$

$\frac{1}{4}(n-1)$ Zahlen vor, welche kleiner als $\frac{1}{2}n$ sind, und diesen entsprechen offenbar positive Sinus; dagegen werden die $\frac{1}{4}(n-1)$ übrigen grösser als $\frac{1}{2}n$ sein, und diesen werden negative Sinus entsprechen. Daher ist das Product aller Sinus gleich dem Producte aus einer positiven Grösse und dem Factor $(-1)^{\frac{1}{4}(n-1)}$ zu setzen, und demnach ist W gleich dem Product aus einer reellen positiven Grösse und dem Factor i^{n-1} oder 1, da $i^4 = 1$ und $n-1$ durch 4 teilbar ist, d. h. W ist eine reelle positive Grösse, so dass notwendig sein muss:

$$W = +\sqrt{n}, \quad T = +\sqrt{n}.$$

In dem andern Falle aber, wo n von der Form $4\mu + 3$ ist, sind in der Reihe der ungeraden Zahlen

$$1, 3, 5, 7, \ldots, \tfrac{1}{2}(n-1), \tfrac{1}{2}(n+3), \ldots, n-2$$

die ersten $\frac{1}{4}(n+1)$ kleiner als $\frac{1}{2}n$, die übrigen $\frac{1}{4}(n-3)$ aber grösser als $\frac{1}{2}n$. Daher werden unter den Sinus der Bogen $\omega, 3\omega, 5\omega, \ldots, (n-2)\omega$ sich $\frac{1}{4}(n-3)$ negative befinden und somit wird W das Product aus $i^{\frac{1}{2}(n-1)}$, einer reellen positiven Grösse und dem Factor $(-1)^{\frac{1}{4}(n-3)}$ sein; der dritte Factor ist gleich $i^{\frac{1}{2}(n-3)}$ und dieser giebt mit dem ersten verbunden $i^{n-2} = i$, da $i^{n-3} = 1$ ist. Mithin ist notwendig:

$$W = +i\sqrt{n} \text{ und } U = +\sqrt{n}.$$

15.

Wir werden nun zeigen, wie eben dieselben Schlüsse aus der im Artikel 9 betrachteten Reihe abgeleitet werden können. Schreiben wir in der Gleichung [4] $-y^{-1}$ für $x^{\frac{1}{2}}$, so folgt:

$$\begin{aligned}[7] \quad & 1 - y^{-1}\frac{1-y^{-2m}}{1-y^{-2}} + y^{-2}\frac{(1-y^{-2m})(1-y^{-2m+2})}{(1-y^{-2})(1-y^{-4})} \\ & - y^{-3}\frac{(1-y^{-2m})(1-y^{-2m+2})(1-y^{-2m+4})}{(1-y^{-2})(1-y^{-4})(1-y^{-6})} + \ldots\ldots \text{bis zum } m+1^{\text{ten}} \text{Gliede} \\ & = (1-y^{-1})(1+y^{-2})(1-y^{-3})(1+y^{-4})\ldots(1 \pm y^{-m}).\end{aligned}$$

Wenn man nun hier für y eine eigentliche Wurzel der Gleichung $y^n - 1 = 0$ nimmt, etwa r, und zugleich $m = n - 1$ setzt, so ist:

$$\frac{1-y^{-2m}}{1-y^{-2}} = \frac{1-r^2}{1-r^{-2}} = -r^2$$
$$\frac{1-y^{-2m+2}}{1-y^{-4}} = \frac{1-r^4}{1-r^{-4}} = -r^4$$
$$\frac{1-y^{-2m+4}}{1-y^{-6}} = \frac{1-r^6}{1-r^{-6}} = -r^6$$
$$\cdots\cdots\cdots\cdots$$
$$\frac{1-y^{-2}}{1-y^{-2m}} = \frac{1-r^{2n-2}}{1-r^{-2n+2}} = -r^{2n-2},$$

wobei zu bemerken ist, dass keiner der Nenner $1-r^{-2}$, $1-r^{-4}$, ... gleich 0 wird. Hiernach nimmt die Gleichung [7] die folgende Form an:

$$1 + r + r^4 + r^9 + \cdots + r^{(n-1)^2} = (1-r^{-1})(1+r^{-2})(1-r^{-3})\cdots(1+r^{-n+1}).$$

Multipliciert man auf der rechten Seite dieser Gleichung den ersten Factor mit dem letzten, den zweiten mit dem vorletzten u. s. w., so erhält man:

$$(1-r^{-1})(1+r^{-n+1}) = r - r^{-1}$$
$$(1+r^{-2})(1-r^{-n+2}) = r^{n-2} - r^{-n+2}$$
$$(1-r^{-3})(1+r^{-n+3}) = r^3 - r^{-3}$$
$$(1+r^{-4})(1-r^{-n+4}) = r^{n-4} - r^{-n+4}$$

u. s. w.

Aus diesen Teilproducten entsteht, wie man leicht sieht, das Product:

$$(r-r^{-1})\,(r^3-r^{-3})\,(r^5-r^{-5})\cdots(r^{n-4}-r^{-n+4})\,(r^{n-2}-r^{-n+2}),$$

und dieses ist daher

$$= 1 + r + r^4 + r^9 + \cdots + r^{(n-1)^2} = W.$$

Diese Gleichung ist identisch mit der aus der ersten Reihe abgeleiteten Gleichung [5] im Artikel 12; aus ihr werden dann die übrigen Schlüsse in derselben Weise abgeleitet wie in den Artikeln 13 und 14.

16.

Wir gehen jetzt zu dem andern Falle, wo n eine gerade Zahl ist, über. Ist zunächst n von der Form $4\mu + 2$ oder eine ungerademal gerade Zahl, so ist klar, dass die Zahlen $\frac{1}{4}n^2$, $(\frac{1}{2}n+1)^2-1$, $(\frac{1}{2}n+2)^2-4$, $\cdots$ oder allgemein $(\frac{1}{2}n+\lambda)^2-\lambda^2$, wenn man sie durch $\frac{1}{2}n$ dividiert, ungerade Quotienten ergeben und somit der Zahl $\frac{1}{2}n$ nach dem

Modul n congruent sein werden. Hieraus folgt, dass, wenn r eine eigentliche Wurzel der Gleichung $x^n - 1 = 0$ und somit $r^{\frac{1}{2}n} = -1$ ist,

$$r^{(\frac{1}{2}n)^2} = -1$$
$$r^{(\frac{1}{2}n+1)^2} = -r$$
$$r^{(\frac{1}{2}n+2)^2} = -r^4$$
$$r^{(\frac{1}{2}n+3)^2} = -r^9$$
u. s. w.

wird. Demnach wird sich in der Reihe

$$1 + r + r^4 + r^9 + \cdots + r^{(n-1)^2}$$

das Glied $r^{(\frac{1}{2}n)^2}$ gegen das erste, das folgende Glied gegen das zweite u. s. w. aufheben, und daher ist:

$$W = 0, \quad T = 0, \quad U = 0.$$

17.

Es bleibt noch der Fall übrig, wo n von der Form 4μ oder eine gerademal gerade Zahl ist. Hier ist allgemein $(\frac{1}{2}n + \lambda)^2 - \lambda^2$ teilbar durch n und daher:

$$r^{(\frac{1}{2}n+\lambda)^2} = r^{\lambda^2}.$$

Demnach ist in der Reihe

$$1 + r + r^4 + r^9 + \cdots + r^{(n-1)^2}$$

das Glied $r^{(\frac{1}{2}n)^2}$ gleich dem ersten, das folgende Glied gleich dem zweiten u. s. w., so dass wird:

$$W = 2(1 + r + r^4 + r^9 + \cdots + r^{(\frac{1}{2}n-1)^2}).$$

Nehmen wir nun an, dass in der Gleichung [7] des Artikels 15 $m = \frac{1}{2}n - 1$ gesetzt und für y eine eigentliche Wurzel der Gleichung $y^n - 1 = 0$, etwa die Wurzel r, genommen werde, so erhält die Gleichung ebenso wie im Artikel 15 die folgende Form:

$$1 + r + r^4 + \cdots + r^{(\frac{1}{2}n-1)^2} = (1 - r^{-1})(1 + r^{-2})(1 - r^{-3}) \cdots (1 - r^{-\frac{1}{2}n+1}),$$

oder:

$$[8] \quad W = 2(1 - r^{-1})(1 + r^{-2})(1 - r^{-3})(1 + r^{-4}) \cdots (1 - r^{-\frac{1}{2}n+1}).$$

Da ferner $r^{\frac{1}{2}n} = -1$ und somit

$$1 + r^{-2} = -r^{\frac{1}{2}n-2}(1 - r^{-\frac{1}{2}n+2})$$
$$1 + r^{-4} = -r^{\frac{1}{2}n-4}(1 - r^{-\frac{1}{2}n+4})$$
$$1 + r^{-6} = -r^{\frac{1}{2}n-6}(1 - r^{-\frac{1}{2}n+6})$$
u. s. w.

ist und das Product aus den Factoren $-r^{\frac{1}{2}n-2}$, $-r^{\frac{1}{2}n-4}$, $-r^{\frac{1}{2}n-6}$, ... bis zu $-r^2$ gleich $(-1)^{\frac{1}{4}n-1}\, r^{\frac{1}{16}n^2-\frac{1}{4}n}$ wird, so lässt sich die vorstehende Gleichung auch so darstellen:

$$W = 2(-1)^{\frac{1}{4}n-1}\, r^{\frac{1}{16}n^2-\frac{1}{4}n}\, (1-r^{-1})(1-r^{-2})(1-r^{-3})(1-r^{-4})\cdots (1-r^{-\frac{1}{2}n+1}).$$

Da man

$$\begin{aligned} 1-r^{-1} &= -r^{-1}(1-r^{-n+1})\\ 1-r^{-2} &= -r^{-2}(1-r^{-n+2})\\ 1-r^{-3} &= -r^{-3}(1-r^{-n+3})\\ &\text{u. s. w.} \end{aligned}$$

hat, so wird:

$$\begin{aligned} &(1-r^{-1})(1-r^{-2})(1-r^{-3})\ldots\ldots(1-r^{-\frac{1}{2}n+1})\\ &= (-1)^{\frac{1}{2}n-1} r^{-\frac{1}{8}n^2+\frac{1}{4}n}(1-r^{-\frac{1}{2}n-1})(1-r^{-\frac{1}{2}n-2})(1-r^{-\frac{1}{2}n-3})\ldots(1-r^{-n+1}), \end{aligned}$$

und daher

$$W = 2(-1)^{\frac{3}{4}n-2} r^{-\frac{1}{16}n^2}(1-r^{-\frac{1}{2}n-1})(1-r^{-\frac{1}{2}n-2})(1-r^{-\frac{1}{2}n-3})\ldots(1-r^{-n+1}).$$

Multipliciert man diesen Wert von W mit dem früher gefundenen und fügt beiderseits den Factor $1-r^{-\frac{1}{2}n}$ hinzu, so ergiebt sich:

$$(1-r^{-\frac{1}{2}n})\, W^2 = 4(-1)^{n-3} r^{-\frac{1}{4}n}(1-r^{-1})(1-r^{-2})(1-r^{-3})\ldots(1-r^{-n+1}).$$

Es ist aber:

$$\begin{aligned} 1-r^{-\frac{1}{2}n} &= 2\\ (-1)^{n-3} &= -1\\ r^{-\frac{1}{4}n} &= -r^{\frac{1}{4}n}\\ (1-r^{-1})(1-r^{-2})(1-r^{-3})\ldots(1-r^{-n+1}) &= n. \end{aligned}$$

Mithin folgt hieraus schliesslich:

[9] $$W^2 = 2r^{\frac{1}{4}n} n.$$

Nun sieht man leicht, dass $r^{\frac{1}{4}n}$ entweder gleich $+i$ oder gleich $-i$ ist, je nachdem nämlich k entweder von der Form $4\mu+1$ oder von der Form $4\mu+3$ ist. Und da

$$2i = (1+i)^2, \quad -2i = (1-i)^2$$

ist, so wird in dem Falle, wo k von der Form $4\mu+1$ ist:

$$W = \pm(1+i)\sqrt{n} \quad \text{und daher } T = U = \pm\sqrt{n},$$

in dem andern Falle aber, wo k von der Form $4\mu+3$ ist:

$$W = \pm(1-i)\sqrt{n} \quad \text{und daher } T = -U = \pm\sqrt{n}.$$

18.

Die Methode des vorigen Artikels hat die absoluten Werte der Functionen T, U geliefert und die Bedingungen ergeben, unter denen jenen gleiche oder entgegengesetzte Vorzeichen beizulegen sind, die Vorzeichen selbst aber sind hierdurch noch nicht bestimmt. Dies ergänzen wir für den Fall, wo $k = 1$ gesetzt wird, in folgender Weise:

Setzen wir $\rho = \cos \frac{1}{2}\omega + i \sin \frac{1}{2}\omega$, so dass $r = \rho^2$ wird, so wird offenbar wegen $\rho^n = -1$ die Gleichung [8] folgendermassen dargestellt werden können:

$$W = 2(1+\rho^{n-2})(1+\rho^{-4})(1+\rho^{n-6})(1+\rho^{-8})\ldots(1+\rho^{-n+4})(1+\rho^{2}),$$

oder, wenn die Factoren in einer anderen Reihenfolge gesetzt werden:

$$W = 2(1+\rho^{2})(1+\rho^{-4})(1+\rho^{6})(1+\rho^{-8})\ldots(1+\rho^{-n+4})(1+\rho^{n-2}).$$

Nun ist:

$$\begin{aligned} 1+\rho^{2} &= 2\rho \cos \tfrac{1}{2}\omega \\ 1+\rho^{-4} &= 2\rho^{-2} \cos \omega \\ 1+\rho^{6} &= 2\rho^{3} \cos \tfrac{3}{2}\omega \\ 1+\rho^{-8} &= 2\rho^{-4} \cos 2\omega \end{aligned}$$

u. s. w.

bis zu

$$\begin{aligned} 1+\rho^{-n+4} &= 2\rho^{-\frac{1}{2}n+2} \cos(\tfrac{1}{4}n-1)\,\omega \\ 1+\rho^{n-2} &= 2\rho^{\frac{1}{2}n-1} \cos(\tfrac{1}{4}n-\tfrac{1}{2})\,\omega. \end{aligned}$$

Daher erhält man:

$$W = 2^{\frac{1}{2}n}\rho^{\frac{1}{4}n} \cos\tfrac{1}{2}\omega \cos\omega \cos\tfrac{3}{2}\omega \cdots \cos(\tfrac{1}{4}n-\tfrac{1}{2})\,\omega.$$

Die in dieses Product eingehenden Cosinus sind offenbar sämtlich positiv, der Factor $\rho^{\frac{1}{4}n}$ aber wird gleich $\cos 45^\circ + i \sin 45^\circ = (1+i)\sqrt{\frac{1}{2}}$. Hieraus folgt, dass W das Product aus $1+i$ in eine reelle positive Grösse ist, wonach notwendig sein muss:

$$W = (1+i)\sqrt{n}, \quad T = +\sqrt{n}, \quad U = +\sqrt{n}.$$

19.

Es wird der Mühe wert sein, alle bisher entwickelten Summationen hier nochmals zusammenzustellen. Allgemein nämlich ist:

$T=$	$U=$	je nachdem n von der Form ist
$\pm\sqrt{n}$	$\pm\sqrt{n}$	4μ
$\pm\sqrt{n}$	0	$4\mu+1$
0	0	$4\mu+2$
0	$\pm\sqrt{n}$	$4\mu+3$,

und in dem Falle, wo $k=1$ vorausgesetzt wird, muss der Wurzelgrösse das positive Vorzeichen beigelegt werden. Daher ist jetzt das, was wir für prime Werte von n im Artikel 3 auf inductivem Wege gefunden hatten, in aller Strenge bewiesen, und es bleibt nur noch übrig zu zeigen, wie man die Vorzeichen für beliebige Werte von k in allen Fällen bestimmen kann. Aber bevor wir diese Aufgabe in der ganzen Allgemeinheit anzugreifen vermögen, müssen wir zunächst diejenigen Fälle, in denen n eine Primzahl oder die Potenz einer Primzahl ist, näher betrachten.

20.

Ist zunächst n eine ungerade Primzahl, so ist offenbar nach dem, was wir im Artikel 10 auseinandergesetzt haben, $W=1+2\Sigma r^a$ $=1+2\Sigma R^{ak}$, wenn $R=\cos\omega+i\sin\omega$ gesetzt wird und a wie dort unbestimmt alle quadratischen Reste von n zwischen 1 und $n-1$ bezeichnet. Wenn man nun ebenso durch b unbestimmt alle quadratischen Nichtreste von n zwischen denselben Grenzen ausdrückt, so sieht man leicht, dass sämtliche Zahlen ak nach dem Modul n entweder sämtlichen a oder sämtlichen b (ohne Rücksicht auf die Reihenfolge) congruent werden, je nachdem k entweder Rest oder Nichtrest ist. Daher wird im ersteren Falle:

$$W=1+2\Sigma R^a=1+R+R^4+R^9+\cdots+R^{(n-1)^2}$$

und daher $W=+\sqrt{n}$, wenn n von der Form $4\mu+1$, und $W=+i\sqrt{n}$, wenn n von der Form $4\mu+3$ ist.

Im andern Falle, wo k Nichtrest von n ist, wird dagegen:

$$W=1+2\Sigma R^b.$$

Hieraus ergiebt sich, da offenbar sämtliche a, b den Complex der ganzen Zahlen $1, 2, 3, \ldots, n-1$ erschöpfen und daher

$$\Sigma R^a+\Sigma R^b=R+R^2+R^3+\cdots+R^{n-1}=-1$$

ist:

$$W=-1-2\Sigma R^a=-(1+R+R^4+R^9+\cdots+R^{(n-1)^2}),$$

und daher $W=-\sqrt{n}$, wenn n von der Form $4\mu+1$, und $W=-i\sqrt{n}$, wenn n von der Form $4\mu+3$ ist.

Hieraus folgt also:

Erstens, wenn n von der Form $4\mu+1$ und k quadratischer Rest von n ist:

$$T=+\sqrt{n},\quad U=0.$$

Zweitens, wenn n von der Form $4\mu+1$ und k quadratischer Nichtrest von n ist:

$$T=-\sqrt{n},\quad U=0.$$

Drittens, wenn n von der Form $4\mu + 3$ und k quadratischer Rest von n ist:

$$T = 0, \qquad U = +\sqrt{n}.$$

Viertens, wenn n von der Form $4\mu + 3$ und k quadratischer Nichtrest von n ist:

$$T = 0, \qquad U = -\sqrt{n}.$$

21.

Es sei zweitens n das Quadrat oder eine höhere Potenz einer ungeraden Primzahl p, und es werde $n = p^{2\varkappa} q$ gesetzt, so dass q entweder gleich 1 oder gleich p ist. Hier wollen wir vor Allem bemerken, dass, wenn λ irgend eine ganze durch $p^{\varkappa}$ nicht teilbare Zahl ist,

$$\begin{aligned} & r^{\lambda^2} + r^{(\lambda+p^{\varkappa}q)^2} + r^{(\lambda+2p^{\varkappa}q)^2} + r^{(\lambda+3p^{\varkappa}q)^2} + \cdots + r^{(\lambda+n-p^{\varkappa}q)^2} \\ &= r^{\lambda^2}\left(1 + r^{2\lambda p^{\varkappa}q} + r^{4\lambda p^{\varkappa}q} + r^{6\lambda p^{\varkappa}q} + \cdots + r^{2\lambda(n-p^{\varkappa}q)}\right) \\ &= r^{\lambda^2}\frac{1 - r^{2\lambda n}}{1 - r^{2\lambda q^{\varkappa}q}} \\ &= 0 \end{aligned}$$

ist. Hieraus ist leicht ersichtlich, dass

$$W = 1 + r^{p^{2\varkappa}} + r^{4p^{2\varkappa}} + r^{9p^{2\varkappa}} + \cdots + r^{(n-p^{\varkappa})^2}$$

wird. Denn die übrigen Glieder der Reihe

$$1 + r + r^4 + r^9 + \cdots + r^{(n-1)^2}$$

können in $(p^{\varkappa} - 1)q$ Teilreihen verteilt werden, von denen jede $p^{\varkappa}$ Glieder enthält und infolge der eben angegebenen Transformation eine verschwindende Summe besitzt.

Hieraus schliesst man, dass in dem Falle, wo $q = 1$ oder n eine Potenz einer Primzahl mit geradem Exponenten ist,

$$W = p^{\varkappa} = +\sqrt{n} \text{ und daher } T = +\sqrt{n},\ U = 0$$

ist.

In dem Falle dagegen, wo $q = p$ oder wo n eine Potenz einer Primzahl mit ungeradem Exponenten ist, setzen wir $r^{p^{2\varkappa}} = \rho$, wonach ρ eine eigentliche Wurzel der Gleichung $x^p - 1 = 0$ ist und zwar $\rho = \cos\frac{k}{p}360° + i\sin\frac{k}{p}360°$, und ferner:

$$W = 1 + \rho + \rho^4 + \rho^9 + \cdots + \rho^{(p^{\varkappa+1}-1)^2} = p^{\varkappa}\left(1 + \rho + \rho^4 + \rho^9 + \cdots + \rho^{(p-1)^2}\right).$$

Die Summe der Reihe $1 + \rho + \rho^4 + \rho^9 + \cdots + \rho^{(p-1)^2}$ aber ist nach dem vorigen Artikel bestimmt, woraus unmittelbar folgt, dass

$$W = \pm \sqrt{n} = T \text{ ist, falls } p \text{ von der Form } 4\mu + 1 \text{ ist,}$$
$$W = \pm i\sqrt{n} = iU \text{ ist, falls } p \text{ von der Form } 4\mu + 3 \text{ ist,}$$

und zwar gilt das positive oder negative Vorzeichen, je nachdem k Rest oder Nichtrest von p ist.

22.

Aus dem, was in den Artikeln 20 und 21 auseinandergesetzt ist, leitet man auch leicht den folgenden Satz ab, der uns später einen bemerkenswerten Nutzen gewähren wird. Setzt man

$$W' = 1 + r^h + r^{4h} + r^{9h} + \cdots + r^{h(n-1)^2},$$

wo h irgend eine ganze durch p nicht teilbare Zahl bezeichnet, so wird in dem Falle, wo $n = p$ oder wo n eine Potenz von p mit ungeradem Exponenten ist,

$$W' = W, \text{ falls } h \text{ quadratischer Rest von } p \text{ ist,}$$
$$W' = -W, \text{ falls } h \text{ quadratischer Nichtrest von } p \text{ ist.}$$

Denn offenbar geht W' aus W hervor, wenn man kh für k substituiert; im ersteren Falle aber sind k und kh gleichartig, im letzteren ungleichartig, insofern nämlich ihre Eigenschaft als Reste oder Nichtreste von p in Betracht kommt.

In dem Falle dagegen, wo n eine Potenz von p mit geradem Exponenten ist, wird offenbar $W' = +\sqrt{n}$ und daher immer $W' = W$.

23.

In den Artikeln 20, 21 und 22 haben wir ungerade Primzahlen und Potenzen von solchen betrachtet; es bleibt daher nur noch der Fall übrig, wo n eine Potenz von 2 ist.

Für $n = 2$ ist offenbar $W = 1 + r = 0$.

Für $n = 4$ ergiebt sich $W = 1 + r + r^4 + r^9 = 2 + 2r$, demnach $W = 2 + 2i$, sooft k von der Form $4\mu + 1$, und $W = 2 - 2i$, sooft k von der Form $4\mu + 3$ ist.

Für $n = 8$ haben wir $W = 1 + r + r^4 + r^9 + r^{16} + r^{25} + r^{36} + r^{49} = 2 + 4r + 2r^4 = 4r$. Demnach ist:

$$W = (1 + i)\sqrt{8}, \text{ sooft } k \text{ von der Form } 8\mu + 1 \text{ ist,}$$
$$W = (-1 + i)\sqrt{8}, \text{ sooft } k \text{ von der Form } 8\mu + 3 \text{ ist,}$$
$$W = (-1 - i)\sqrt{8}, \text{ sooft } k \text{ von der Form } 8\mu + 5 \text{ ist,}$$
$$W = (1 - i)\sqrt{8}, \text{ sooft } k \text{ von der Form } 8\mu + 7 \text{ ist.}$$

Ist n eine höhere Potenz von 2, so setzen wir $n = 2^{2\varkappa} q$, so dass q entweder gleich 1 oder gleich 2 und $\varkappa$ grösser als 1 ist. Hier muss man vor Allem bemerken, dass, wenn λ irgend eine durch $2^{\varkappa-1}$ nicht teilbare ganze Zahl ist,

$$\begin{aligned} & r^{\lambda^2} + r^{(\lambda+2^\varkappa q)^2} + r^{(\lambda+2\cdot 2^\varkappa q)^2} + r^{(\lambda+3\cdot 2^\varkappa q)^2} + \cdots + r^{(\lambda+n-2^\varkappa q)^2} \\ & = r^{\lambda^2}\left\{1 + r^{2^{\varkappa+1}\lambda q} + r^{2\cdot 2^{\varkappa+1}\lambda q} + r^{3\cdot 2^{\varkappa+1}\lambda q} + \cdots + r^{(2n-2^{\varkappa+1}q)\lambda}\right\} \\ & = r^{\lambda^2} \frac{1 - r^{2\lambda n}}{1 - r^{2^{\varkappa+1}\lambda q}} \\ & = 0 \end{aligned}$$

wird. Hieraus ist leicht ersichtlich, dass

$$W = 1 + r^{2^{2\varkappa-2}} + r^{4\cdot 2^{2\varkappa-2}} + r^{9\cdot 2^{2\varkappa-2}} + \cdots + r^{(n-2^{\varkappa-1})^2}$$

wird.

Setzen wir $r^{2^{2\varkappa-2}} = \rho$, so ist ρ eine Wurzel der Gleichung $x^{4q} - 1 = 0$ und zwar $\rho = \cos\frac{k}{4q} 360° + i \sin\frac{k}{4q} 360°$. Sodann wird:

$$\begin{aligned} W &= 1 + \rho + \rho^4 + \rho^9 + \cdots + \rho^{(2^{\varkappa+1}q-1)^2} \\ &= 2^{\varkappa-1}(1 + \rho + \rho^4 + \rho^9 + \cdots + \rho^{(4q-1)^2}). \end{aligned}$$

Die Summe der Reihe $1 + \rho + \rho^4 + \rho^9 + \cdots + \rho^{(4q-1)^2}$ wird aber durch das, was über die Fälle $n = 4$, $n = 8$ dargelegt wurde, bestimmt; somit ergiebt sich in dem Falle, wo $q = 1$ oder wo n eine Potenz der Zahl 4 ist:

$$\begin{aligned} W &= (1 + i)\, 2^\varkappa = (1 + i)\sqrt{n}, \text{ falls } k \text{ von der Form } 4\mu + 1 \text{ ist,} \\ W &= (1 - i)\, 2^\varkappa = (1 - i)\sqrt{n}, \text{ falls } k \text{ von der Form } 4\mu + 3 \text{ ist,} \end{aligned}$$

Formeln, welche genau mit den für $n = 4$ angegebenen übereinstimmen; in dem Falle aber, wo $q = 2$ oder n eine Potenz von 2 mit einem ungeraden die Zahl 3 übersteigenden Exponenten ist:

$$\begin{aligned} W &= (1 + i)\, 2^\varkappa \sqrt{2} = (1 + i)\sqrt{n}, \text{ falls } k \text{ von der Form } 8\mu + 1 \text{ ist,} \\ W &= (-1 + i)\, 2^\varkappa \sqrt{2} = (-1 + i)\sqrt{n}, \text{ falls } k \text{ von der Form } 8\mu + 3 \text{ ist,} \\ W &= (-1 - i)\, 2^\varkappa \sqrt{2} = (-1 - i)\sqrt{n}, \text{ falls } k \text{ von der Form } 8\mu + 5 \text{ ist,} \\ W &= (1 - i)\, 2^\varkappa \sqrt{2} = (1 - i)\sqrt{n}, \text{ falls } k \text{ von der Form } 8\mu + 7 \text{ ist,} \end{aligned}$$

und diese Formeln stimmen ebenfalls vollkommen mit denen überein, welche wir für $n = 8$ angegeben haben.

24.

Auch hier wird es sich der Mühe lohnen, das Verhältnis zu bestimmen, in welchem die Summe der Reihe

$$W' = 1 + r^h + r^{4h} + r^{9h} + \cdots + r^{h(n-1)^2},$$

wo h irgend eine ungerade ganze Zahl bezeichnet, zu W steht. Da W' aus W entsteht, wenn man k in kh verwandelt, so wird der Wert von W' ebenso von der Form der Zahl kh abhängen, wie W von der Form von k. Setzt man $\frac{W'}{W} = l$, so wird offenbar:

I. in dem Falle, wo $n = 4$ oder eine höhere Potenz von 2 mit geradem Exponenten ist:

$l = 1$, wenn h von der Form $4\mu + 1$ ist,
$l = -i$, wenn h von der Form $4\mu + 3$ und k von der Form $4\mu + 1$ ist,
$l = +i$, wenn h von der Form $4\mu + 3$ und k von derselben Form ist;

II. in dem Falle, wo $n = 8$ oder eine höhere Potenz von 2 mit ungeradem Exponenten ist:

$l = 1$, wenn h von der Form $8\mu + 1$ ist,
$l = -1$, wenn h von der Form $8\mu + 5$ ist,
$l = +i$, wenn entweder h von der Form $8\mu + 3$ und k von der Form $4\mu + 1$,
oder h von der Form $8\mu + 7$ und k von der Form $4\mu + 3$ ist,
$l = -i$, wenn entweder h von der Form $8\mu + 3$ und k von der Form $4\mu + 3$
oder h von der Form $8\mu + 7$ und k von der Form $4\mu + 1$ ist.

Durch das Vorhergehende ist die Bestimmung der Summe W für diejenigen Fälle, in denen n eine Primzahl oder eine Potenz einer Primzahl ist, vollständig durchgeführt; es bleiben daher nur noch diejenigen Fälle zu erledigen, in denen n aus mehreren Primzahlen zusammengesetzt ist. Hierzu bahnt uns der folgende Satz den Weg.

25.

Satz. Ist n das Product aus **zwei** ganzen positiven zu einander primen Zahlen a, b und setzt man:

$$P = 1 + r^{a^2} + r^{4a^2} + r^{9a^2} + \cdots + r^{(b-1)^2a^2}$$
$$Q = 1 + r^{b^2} + r^{4b^2} + r^{9b^2} + \cdots + r^{(a-1)^2b^2},$$

so behaupte ich, dass $W = PQ$ ist.

Beweis. Bezeichnet α unbestimmt die Zahlen $0, 1, 2, 3, \ldots, a-1$, β unbestimmt die Zahlen $0, 1, 2, 3, \ldots, b-1$, ν unbestimmt die Zahlen $0, 1, 2, 3, \ldots, n-1$, so ist offenbar:

$$P = \Sigma r^{a^2\beta^2}, \quad Q = \Sigma r^{b^2\alpha^2}, \quad W = \Sigma r^{\nu^2}.$$

Hiernach ist $PQ = \Sigma r^{a^2\beta^2 + b^2\alpha^2}$, wenn man für α und β alle Werte in allen

möglichen Verbindungen setzt; wegen $2ab\alpha\beta = 2\alpha\beta n$ ist ferner $PQ = \Sigma r^{(a\beta+b\alpha)^2}$. Man sieht aber ohne Schwierigkeit, dass die einzelnen Werte von $a\beta + b\alpha$ unter einander verschieden und irgend einem Werte von ν gleich sind. Demnach ist $PQ = \Sigma r^{\nu^2} = W$.

Übrigens ist zu bemerken, dass r^{a^2} eine eigentliche Wurzel der Gleichung $x^b - 1 = 0$ und r^{b^2} eine eigentliche Wurzel der Gleichung $x^a - 1 = 0$ ist.

26.

Ist ferner n das Product aus drei zu einander primen Zahlen a, b, c, so werden offenbar, wenn man $bc = b'$ setzt, auch a und b' prim zu einander sein; und daher ist W das Product aus den beiden Factoren:

$$1 + r^{a^2} + r^{4a^2} + r^{9a^2} + \cdots + r^{(b'-1)^2a^2}$$
$$1 + r^{b'^2} + r^{4b'^2} + r^{9b'^2} + \cdots + r^{(a-1)^2b'^2}.$$

Da aber r^{a^2} eine eigentliche Wurzel der Gleichung $x^{bc} - 1 = 0$ ist, so ist der erste Factor selbst das Product aus

$$1 + \rho^{b^2} + \rho^{4b^2} + \rho^{9b^2} + \cdots + \rho^{(c-1)^2b^2}$$
$$1 + \rho^{c^2} + \rho^{4c^2} + \rho^{9c^2} + \cdots + \rho^{(b-1)^2c^2},$$

wenn man $r^{a^2} = \rho$ setzt. Hieraus geht hervor, dass W das Product aus den drei Factoren ist:

$$1 + r^{b^2c^2} + r^{4b^2c^2} + r^{9b^2c^2} + \cdots + r^{(a-1)^2b^2c^2}$$
$$1 + r^{a^2c^2} + r^{4a^2c^2} + r^{9a^2c^2} + \cdots + r^{(b-1)^2a^2c^2}$$
$$1 + r^{a^2b^2} + r^{4a^2b^2} + r^{9a^2b^2} + \cdots + r^{(c-1)^2a^2b^2},$$

wo $r^{b^2c^2}, r^{a^2c^2}, r^{a^2b^2}$ respective eigentliche Wurzeln der Gleichungen $x^a - 1 = 0$, $x^b - 1 = 0$, $x^c - 1 = 0$ sind.

27.

Hieraus schliesst man leicht allgemein, dass, wenn n das Product aus beliebig vielen zu einander primen Factoren $a, b, c, \ldots$ ist, W das Product aus ebensovielen Factoren ist, und zwar sind diese letzteren:

$$1 + r^{\frac{n^2}{a^2}} + r^{\frac{4n^2}{a^2}} + r^{\frac{9n^2}{a^2}} + \cdots + r^{\frac{(a-1)^2n^2}{a^2}}$$
$$1 + r^{\frac{n^2}{b^2}} + r^{\frac{4n^2}{b^2}} + r^{\frac{9n^2}{b^2}} + \cdots + r^{\frac{(b-1)^2n^2}{b^2}}$$
$$1 + r^{\frac{n^2}{c^2}} + r^{\frac{4n^2}{c^2}} + r^{\frac{9n^2}{c^2}} + \cdots + r^{\frac{(c-1)^2n^2}{c^2}}$$
$$\cdots\cdots\cdots\cdots\cdots,$$

wo $r^{\frac{n^2}{a^2}}, r^{\frac{n^2}{b^2}}, r^{\frac{n^2}{c^2}}, \ldots$ eigentliche Wurzeln respective von den Gleichungen $x^a - 1 = 0$, $x^b - 1 = 0$, $x^c - 1 = 0, \ldots$ sind.

28.

Diesen Prinzipien zufolge ist der Übergang zur vollständigen Bestimmung von W für jeden beliebigen Wert von n schon von selbst klar. Man zerlege nämlich n in Factoren $a, b, c, \ldots$, welche entweder ungleiche Primzahlen oder Potenzen ungleicher Primzahlen sind, und setze $r^{\frac{n^2}{a^2}} = A$, $r^{\frac{n^2}{b^2}} = B$, $r^{\frac{n^2}{c^2}} = C, \ldots$ Dann sind $A, B, C, \ldots$ eigentliche Wurzeln der Gleichungen $x^a - 1 = 0$, $x^b - 1 = 0$, $x^c - 1 = 0, \cdots$ und W das Product aus den Factoren:

$$1 + A + A^4 + A^9 + \cdots + A^{(a-1)^2}$$
$$1 + B + B^4 + B^9 + \cdots + B^{(b-1)^2}$$
$$1 + C + C^4 + C^9 + \cdots + C^{(c-1)^2}$$

u. s. w.

Jeder dieser Factoren aber lässt sich nach dem, was wir in den Artikeln 20, 21 und 23 dargelegt haben, bestimmen, so dass hiernach auch der Wert des Products bekannt ist. Es dürfte nicht unnützlich sein, die Regeln für die Bestimmung jener Factoren hier zusammenzustellen, damit man sie alle gleichzeitig vor sich habe. Da die Wurzel $A = \frac{kn}{a} \cdot \frac{360°}{a}$ ist, so wird sich das Aggregat $1 + A + A^4 + A^9 + \cdots + A^{(a-1)^2}$, welches wir mit L bezeichnen wollen, durch die Zahl $\frac{kn}{a}$ ebenso bestimmen, wie in unsrer allgemeinen Untersuchung W durch die Zahl k. Nun sind zwölf Fälle zu unterscheiden.

I. Ist a eine Primzahl von der Form $4\mu + 1$, etwa gleich p, oder eine Potenz einer solchen Primzahl mit ungeradem Exponenten und zugleich $\frac{kn}{a}$ quadratischer Rest von p, so wird $L = +\sqrt{a}$.

II. Wenn unter sonst gleichen Voraussetzungen $\frac{kn}{a}$ quadratischer Nichtrest von p ist, so wird $L = -\sqrt{a}$.

III. Ist a eine Primzahl von der Form $4\mu + 3$, etwa gleich p, oder eine Potenz einer solchen Primzahl mit ungeradem Exponenten und zugleich $\frac{kn}{a}$ quadratischer Rest von p, so wird $L = +i\sqrt{a}$.

IV. Wenn unter sonst gleichen Voraussetzungen wie in III $\frac{kn}{a}$ quadratischer Nichtrest von p, so wird $L = -i\sqrt{a}$.

V. Ist a ein Quadrat oder eine höhere Potenz einer (ungeraden) Primzahl mit geradem Exponenten, so ist $L = +\sqrt{a}$.

VI. Ist $a = 2$, so ist $L = 0$.

VII. Ist $a=4$ oder eine höhere Potenz von 2 mit geradem Exponenten und ist zugleich $\frac{kn}{a}$ von der Form $4\mu+1$, so ist $L=(1+i)\sqrt{a}$.

VIII. Wenn unter sonst gleichen Voraussetzungen wie in VII $\frac{kn}{a}$ von von der Form $4\mu+3$ ist, so ist $L=(1-i)\sqrt{a}$.

IX. Ist $a=8$ oder eine höhere Potenz von 2 mit ungeradem Exponenten und ist zugleich $\frac{kn}{a}$ von der Form $8\mu+1$ so ist $L=(1+i)\sqrt{a}$.

X. Ist unter sonst gleichen Voraussetzungen wie in IX $\frac{kn}{a}$ von der Form $8\mu+3$, so ist $L=(-1+i)\sqrt{a}$.

XI. Ist unter sonst gleichen Voraussetzungen $\frac{kn}{a}$ von der Form $8\mu+5$, so ist $L=(-1-i)\sqrt{a}$.

XII. Ist unter sonst gleichen Voraussetzungen $\frac{kn}{a}$ von der Form $8\mu+7$, so ist $L=(1-i)\sqrt{a}$.

29.

Es sei **Beispiels** halber $n=2520=8\cdot9\cdot5\cdot7$ und $k=13$. Hier wird:
für $a=8$ nach Fall XII: $L=(1-i)\sqrt{8}$;
für den Factor 9 ist nach Fall V die entsprechende Summe gleich $\sqrt{9}$,
für den Factor 5 ist nach Fall II die entsprechende Summe gleich $-\sqrt{5}$,
für den Factor 7 ist nach Fall III die entsprechende Summe gleich $+i\sqrt{7}$.
Demnach wird $W=(1-i)(-i)\sqrt{2520}=(-1-i)\sqrt{2520}$.

Ist für denselben Wert von n $k=1$, so entspricht
dem Factor 8 die Summe $(-1+i)\sqrt{8}$,
dem Factor 9 die Summe $\sqrt{9}$,
dem Factor 5 die Summe $\sqrt{5}$,
dem Factor 7 die Summe $-i\sqrt{7}$.
Demnach ergiebt sich das Product $W=(1+i)\sqrt{2520}$.

30.

Eine andere Methode, die Summe W allgemein zu bestimmen, gründet sich auf das, was wir in den Artikeln 22 und 24 auseinandergesetzt haben. Setzen wir allgemein $\cos\omega+i\sin\omega=\rho$ und

$$\rho^{\frac{n^2}{a^2}}=\alpha,\quad \rho^{\frac{n^2}{b^2}}=\beta,\quad \rho^{\frac{n^2}{c^2}}=\gamma,\ \ldots,$$

so dass man $r=\rho^k$, $A=\alpha^k$, $B=\beta^k$, $C=\gamma^k$, ... hat, so wird

$$1+\rho+\rho^4+\rho^9+\cdots+\rho^{(n-1)^2}$$

das Product aus den Factoren:

$$1 + \alpha + \alpha^4 + \alpha^9 + \cdots + \alpha^{(a-1)^2}$$
$$1 + \beta + \beta^4 + \beta^9 + \cdots + \beta^{(b-1)^2}$$
$$1 + \gamma + \gamma^4 + \gamma^9 + \cdots + \gamma^{(c-1)^2}$$
$$\cdots\cdots\cdots,$$

und somit W das Product aus den Factoren:

$$w = 1 + \rho + \rho^4 + \rho^9 + \cdots + \rho^{(n-1)^2}$$
$$\mathfrak{A} = \frac{1 + A + A^4 + A^9 + \cdots + A^{(a-1)^2}}{1 + \alpha + \alpha^4 + \alpha^9 + \cdots + \alpha^{(a-1)^2}}$$
$$\mathfrak{B} = \frac{1 + B + B^4 + B^9 + \cdots + B^{(b-1)^2}}{1 + \beta + \beta^4 + \beta^9 + \cdots + \beta^{(b-1)^2}}$$
$$\mathfrak{C} = \frac{1 + C + C^4 + C^9 + \cdots + C^{(c-1)^2}}{1 + \gamma + \gamma^4 + \gamma^9 + \cdots + \gamma^{(c-1)^2}}$$
$$\cdots\cdots\cdots$$

Nun ist der erste Factor w bestimmt durch die oben im Artikel 19 dargelegten Untersuchungen, die übrigen Factoren aber ergeben sich aus den Formeln der Artikel 22 und 24, die wir hier, um sie alle beisammen zu haben, nochmals zusammenstellen.*) Hier sind zwölf Fälle zu unterscheiden, nämlich

I. Ist a eine (ungerade) Primzahl, gleich p, oder eine Potenz einer solchen Primzahl mit ungeradem Exponenten und k quadratischer Rest von p, so ist der entsprechende Factor $\mathfrak{A} = +1$.

II. Ist unter sonst gleichen Voraussetzungen k quadratischer Nichtrest von p, so ist $\mathfrak{A} = -1$.

III. Ist a das Quadrat einer ungeraden Primzahl oder eine höhere Potenz einer solchen mit geradem Exponenten, so ist $\mathfrak{A} = +1$.

IV. Ist $a = 4$ oder eine höhere Potenz von 2 mit geradem Exponenten und zugleich k von der Form $4\mu + 1$, so ist $\mathfrak{A} = +1$.

V. Ist unter sonst gleichen Voraussetzungen wie in IV k von der Form $4\mu + 3$ und $\frac{n}{a}$ von der Form $4\mu + 1$, so ist $\mathfrak{A} = -i$.

VI. Ist unter sonst gleichen Voraussetzungen wie in IV k von der Form $4\mu + 3$ und $\frac{n}{a}$ von der Form $4\mu + 3$, so ist $\mathfrak{A} = +i$.

*) Offenbar ist das, was dort k und h waren, hier $\frac{n}{a}$ und k hinsichtlich des zweiten Factors, $\frac{n}{b}$ und k hinsichtlich des dritten Factors, u. s. w.

VII. Ist $a=8$ oder eine höhere Potenz von 2 mit ungeradem Exponenten und ist k von der Form $8\mu+1$, so ist $\mathfrak{A}=+1$.

VIII. Ist unter sonst gleichen Voraussetzungen wie in VII k von der Form $8\mu+5$, so ist $\mathfrak{A}=-1$.

IX. Ist unter sonst gleichen Voraussetzungen wie in VII k von der Form $8\mu+3$ und $\frac{n}{a}$ von der Form $4\mu+1$, so ist $\mathfrak{A}=+i$.

X. Ist unter sonst gleichen Voraussetzungen wie in VII k von der Form $8\mu+3$ und $\frac{n}{a}$ von der Form $4\mu+3$, so ist $\mathfrak{A}=-i$.

XI. Ist unter sonst gleichen Voraussetzungen wie in VII k von der Form $8\mu+7$ und $\frac{n}{a}$ von der Form $4\mu+1$, so ist $\mathfrak{A}=-i$.

XII. Ist unter sonst gleichen Voraussetzungen wie in VII k von der Form $8\mu+7$ und $\frac{n}{a}$ von der Form $4\mu+3$, so ist $\mathfrak{A}=+i$.

Den Fall, wo $a=2$ ist, übergehen wir; obwohl hier $\mathfrak{A}=\frac{0}{0}$ oder unbestimmt sein würde, ist doch stets $W=0$.

Die übrigen Factoren $\mathfrak{B}, \mathfrak{C}, \ldots$ hängen von $b, c, \ldots$ in derselben Weise ab, wie $\mathfrak{A}$ von a, soweit sie nämlich in die Bestimmung jener eingehen.

31.

Nach dieser zweiten Methode verhält sich das erste Beispiel im Artikel 29 folgendermassen:

Der Factor w wird gleich $(1+i)\sqrt{2520}$.
Für $a=8$ ist nach Fall VIII der entsprechende Factor $\mathfrak{A}=-1$.
Dem zweiten Factor 9 von n entspricht nach Fall III der Factor $+1$.
Dem Factor 5 entspricht der Factor -1 (nach Fall II).
Dem Factor 7 entspricht der Factor -1 (nach Fall II).

Daraus ergiebt sich das Product $W=(-1-i)\sqrt{2520}$, wie im Artikel 29.

32.

Da der Wert von W vermittelst zweier Methoden bestimmt werden kann, von denen die eine sich auf die Beziehungen der Zahlen $\frac{nk}{a}, \frac{nk}{b}, \frac{nk}{c}, \ldots$ zu den Zahlen $a, b, c, \ldots$ gründet, die andere aber von den Beziehungen der Zahl k zu den Zahlen $a, b, c, \ldots$ abhängt, so muss zwischen allen diesen Beziehungen ein gewisser Conditionalzusammenhang stattfinden in der Weise, dass eine jede aus den übrigen bestimmbar sein muss. Wir nehmen an, dass alle Zahlen $a, b, c, \ldots$ ungerade Primzahlen seien und $k=1$ genommen werde; ferner verteilen wir die Factoren $a, b, c, \ldots$ in zwei Klassen, von denen die eine diejenigen enthält, welche von der

Form $4\mu+1$ sind und die mit $p, p', p'', \ldots$ bezeichnet sein mögen, die andere aber aus denen besteht, welche von der Form $4\mu+3$ sind und die durch $q, q', q'', \ldots$ dargestellt werden mögen. Die Anzahl der letzteren bezeichnen wir mit m. Nachdem dies geschehen, bemerken wir, dass n von der Form $4\mu+1$ wird, wenn m gerade ist (hierher muss auch der Fall gerechnet werden, wo Factoren der zweiten Klasse überhaupt nicht vorhanden sind also $m=0$ ist), dass dagegen n von der Form $4\mu+3$ wird, wenn m ungerade ist. Nun wird die Bestimmung von W nach der ersten Methode folgendermassen geleistet. Es mögen die Zahlen $P, P', P'', \ldots, Q, Q', Q'', \ldots$ in der Weise von den Relationen der Zahlen $\frac{n}{p}, \frac{n}{p'}, \frac{n}{p''}, \ldots, \frac{n}{q}, \frac{n}{q'}, \frac{n}{q''}, \ldots$ zu den Zahlen $p, p', p'', \ldots, q, q', q'', \ldots$ respective abhängen, dass

$$P=+1 \text{ ist, wenn } \frac{n}{p} \text{ quadratischer Rest von } p \text{ ist,}$$

$$P=-1 \text{ ist, wenn } \frac{n}{p} \text{ quadratischer Nichtrest von } p \text{ ist,}$$

und ebenso in Bezug auf die übrigen. Dann ist W das Product aus den Factoren $P\sqrt{p}, P'\sqrt{p'}, P''\sqrt{p''}, \ldots, iQ\sqrt{q}, iQ'\sqrt{q'}, iQ''\sqrt{q''}, \ldots$ und daher:

$$W=PP'P''\cdots QQ'Q''\cdots i^m\sqrt{n}.$$

Nach der zweiten Methode oder vielmehr unmittelbar nach den Regeln des Artikels 19 ist:

$W=+\sqrt{n}$, wenn n von der Form $4\mu+1$, oder, was auf dasselbe hinauskommt, wenn m gerade,

$W=+i\sqrt{n}$, wenn n von der Form $4\mu+3$, oder wenn m ungerade ist.

Beide Fälle kann man gleichzeitig umfassen durch die folgende Formel:

$$W=i^{m^2}\sqrt{n}.$$

Demnach folgt also:

$$PP'P''\cdots QQ'Q''\cdots=i^{m^2-m}.$$

Nun ist aber $i^{m^2-m}=1$, sooft m von der Form 4μ oder $4\mu+1$, und $=-1$, sooft m von der Form $4\mu+2$ oder $4\mu+3$ ist; somit erhalten wir den sehr eleganten

Satz. Bezeichnen $a, b, c, \ldots$ ungleiche positive ungerade Primzahlen, deren Product gleich n gesetzt werde und unter denen m von der Form $4\mu+3$, die übrigen aber von der Form

$4\mu + 1$ sind, so ist die Anzahl derjenigen von diesen Zahlen $a, b, c \ldots$, von denen respective $\frac{n}{a}, \frac{n}{b}, \frac{n}{c}, \cdots$ Nichtreste sind, gerade, sooft m von der Form 4μ oder $4\mu + 1$ ist, dagegen ungerade, sooft m von der Form $4\mu + 2$ oder $4\mu + 3$ ist.

So hat man z. B., wenn man $a = 3, b = 5, c = 7, d = 11$ setzt, drei Zahlen von der Form $4\mu + 3$, nämlich 3, 7 und 11. Es ist aber $5 \cdot 7 \cdot 11 R 3$; $3 \cdot 7 \cdot 11 R 5$; $3 \cdot 5 \cdot 11 R 7$; $3 \cdot 5 \cdot 7 N 11$, oder es ist nur allein $\frac{n}{d}$ Nichtrest von d.

33.

Das berühmte **Fundamentaltheorem** über die quadratischen Reste ist nichts anderes, als ein **specieller Fall** des soeben entwickelten Satzes. Beschränkt man nämlich die Anzahl der Zahlen $a, b, c, \ldots$ auf zwei, so wird offenbar, wenn nur eine von ihnen oder keine von der Form $4\mu + 3$ ist, entweder gleichzeitig aRb, bRa oder gleichzeitig aNb, bNa sein müssen; sind dagegen beide von der Form $4\mu + 3$, so wird eine von ihnen Nichtrest der andern und letztere Rest von jener sein müssen. Wir haben also hier einen **vierten** Beweis dieses höchstwichtigen Satzes, von welchem wir einen ersten und zweiten Beweis in den „*Arithmetischen Untersuchungen*“, einen dritten neulich in einer besonderen Abhandlung (*Commentt. T. XVI*, vgl. oben S. 457) mitgeteilt haben; zwei andere, die sich wiederum auf ganz verschiedene Prinzipien stützen, werden wir späterhin auseinandersetzen. Man muss sich höchlichst wundern, dass dieser schöne Satz, welcher zuerst allen Bemühungen, ihn zu beweisen, so hartnäckig spottete, nachher sich auf so vielen gänzlich von einander verschiedenen Wegen zugänglich zeigte.

34.

Auch die übrigen Sätze, welche gleichsam die Ergänzung zum Fundamentaltheorem bilden, nach denen nämlich die Primzahlen erkannt werden, deren Reste oder Nichtreste -1, $+2$ und -2 sind, lassen sich aus denselben Prinzipien ableiten. Wir beginnen mit dem Reste $+2$.

Setzt man $n = 8a$, so dass a eine Primzahl ist, und $k = 1$, so wird der Methode des Artikels 28 zufolge W das Product aus zwei Factoren, von denen der eine $+\sqrt{a}$ oder $+i\sqrt{a}$ ist, wenn 8 oder, was dasselbe ist, 2 quadratischer Rest von a ist, dagegen $-\sqrt{a}$ oder $-i\sqrt{a}$, wenn 2 Nichtrest von a ist. Der andere Factor aber ist

$$(1 + i)\sqrt{8}, \text{ wenn } a \text{ von der Form } 8\mu + 1 \text{ ist;}$$
$$(-1 + i)\sqrt{8}, \text{ wenn } a \text{ von der Form } 8\mu + 3 \text{ ist;}$$
$$(-1 - i)\sqrt{8}, \text{ wenn } a \text{ von der Form } 8\mu + 5 \text{ ist;}$$
$$(1 - i)\sqrt{8}, \text{ wenn } a \text{ von der Form } 8\mu + 7 \text{ ist.}$$

Nach Artikel 18 ist aber immer $W = (1+i)\sqrt{n}$; dividiert man diesen Wert durch die vier Werte des zweiten Factors, so wird offenbar der erste Factor werden müssen:

$$+\sqrt{a}, \text{ wenn } a \text{ von der Form } 8\mu+1 \text{ ist;}$$
$$-i\sqrt{a}, \text{ wenn } a \text{ von der Form } 8\mu+3 \text{ ist;}$$
$$-\sqrt{a}, \text{ wenn } a \text{ von der Form } 8\mu+5 \text{ ist;}$$
$$+i\sqrt{a}, \text{ wenn } a \text{ von der Form } 8\mu+7 \text{ ist.}$$

Hieraus folgt unmittelbar, dass im ersten und vierten Falle 2 Rest von a, im zweiten und dritten Falle aber Nichtrest von a sein muss.

35.

Die Primzahlen, deren Rest oder Nichtrest -1 ist, werden leicht erkannt mit Hülfe des folgenden Satzes, welcher auch an sich merkwürdig genug ist.

Satz. Das Product aus den beiden Factoren

$$W' = 1 + r^{-1} + r^{-4} + \cdots + r^{-(n-1)^2}$$
$$W = 1 + r + r^4 + \cdots + r^{(n-1)^2}$$

ist gleich n, wenn n ungerade, oder gleich 0, wenn n ungerademal gerade, oder gleich $2n$, wenn n gerademal gerade ist.

Beweis. Da offenbar

$$\begin{aligned} W &= r + r^4 + r^9 + \cdots + r^{n^2} \\ &= r^4 + r^9 + \cdots\cdots + r^{(n+1)^2} \\ &= r^9 + r^{16} + \cdots\cdots + r^{(n+2)^2} \\ &\text{u. s. w.} \end{aligned}$$

ist, so lässt sich das Product WW' auch folgendermassen darstellen:

$$\begin{aligned} &1 + r + r^4 + r^9 + \cdots + r^{(n-1)^2} \\ &+ r^{-1}(r + r^4 + r^9 + r^{16} + \cdots + r^{n^2}) \\ &+ r^{-4}(r^4 + r^9 + r^{16} + r^{25} + \cdots + r^{(n+1)^2}) \\ &+ r^{-9}(r^9 + r^{16} + r^{25} + r^{36} + \cdots + r^{(n+2)^2}) \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ &+ r^{-(n-1)^2}(r^{(n-1)^2} + r^{n^2} + r^{(n+1)^2} + r^{(n+2)^2} + \cdots + r^{(2n-2)^2}), \end{aligned}$$

und dieses Aggregat giebt, wenn man die vertikalen Reihen summiert:

$$\begin{aligned} &n \\ &+ r\,(1 + r^2 + r^4 + r^6 + \cdots + r^{2n-2}) \\ &+ r^4(1 + r^4 + r^8 + r^{12} + \cdots + r^{4n-4}) \\ &+ r^9(1 + r^6 + r^{12} + r^{18} + \cdots + r^{6n-6}) \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ &+ r^{(n-1)^2}(1 + r^{2n-2} + r^{4n-4} + r^{6n-6} + \cdots + r^{2(n-1)^2}). \end{aligned}$$

Wenn nun n ungerade ist, so sind die einzelnen Teile dieses Aggregates, ausser dem ersten n, gleich 0; denn der zweite wird offenbar gleich $\frac{r(1-r^{2n})}{1-r^2}$, der dritte gleich $\frac{r^4(1-r^{4n})}{1-r^4}$, u. s. w. Ist aber n gerade, so muss man auch noch den Teil

$$r^{\frac{1}{4}n^2}(1+r^n+r^{2n}+r^{3n}+\cdots+r^{n^2-n}),$$

welcher gleich $nr^{\frac{1}{4}n^2}$ wird, ausnehmen. Im ersten Falle also wird $WW'=n$, im zweiten aber $=n+nr^{\frac{1}{4}n^2}$; es ist aber $r^{\frac{1}{4}n^2}=+1$, wenn n gerademal gerade ist, dann wird also $WW'=2n$; dagegen ist $r^{\frac{1}{4}n^2}=-1$, wenn n ungerademal gerade ist; in diesem Falle ist also $WW'=0$.

36.

Nun weiss man aus Artikel 22, dass, wenn n eine ungerade Primzahl ist, $\frac{W'}{W}=+1$ oder $=-1$ wird, je nachdem -1 Rest oder Nichtrest von n ist. Daher muss in dem ersteren Falle $W^2=+n$, im letzteren $W^2=-n$ sein. Daher schliessen wir nach Artikel 13, dass der erstere Fall nur dann stattfinden kann, wenn n von der Form $4\mu+1$, der letztere aber nur dann, wenn n von der Form $4\mu+3$ ist.

Endlich folgt aus der Combination der für die Reste $+2$ und -1 gefundenen Bedingungen ohne Weiteres, dass -2 Rest einer jeden Primzahl von der Form $8\mu+1$ oder $8\mu+3$ und Nichtrest einer jeden Primzahl von der Form $8\mu+5$ oder $8\mu+7$ ist.

Neue Beweise und Erweiterungen des Fundamentalsatzes in der Lehre von den quadratischen Resten.

(Commentationes soc. reg. sc. Gotting. recentiores, Vol. IV, Gotting. 1818.)

Der Fundamentalsatz über die quadratischen Reste, welcher zu den schönsten Wahrheiten der höheren Arithmetik gehört, ist zwar leicht durch Induction gefunden worden, bei weitem schwieriger aber war es, ihn zu beweisen. Bei derartigen Untersuchungen pflegt es häufiger zu geschehen, dass die Beweise der einfachsten Wahrheiten, die sich dem Forscher auf inductivem Wege gewissermassen von selbst darbieten, sehr tief verborgen liegen und erst nach vielen vergeblichen Versuchen auf ganz anderem Wege, als man sie suchte, endlich ans Tageslicht gefördert werden können. Ferner geschieht es nicht selten, dass, sobald einmal ein Weg gefunden worden ist, sich gleich darauf mehrere Wege eröffnen, welche zu demselben Ziele führen, die einen kürzer und directer, die andern gleichsam von der Seite kommend und von ganz verschiedenen Prinzipien ausgehend, zwischen denen und der vorliegenden Untersuchung man kaum irgend einen Zusammenhang vermutet hätte. Ein solcher wunderbarer Zusammenhang zwischen versteckter liegenden Wahrheiten giebt diesen Betrachtungen nicht nur einen gewissen eigentümlichen Reiz, sondern verdient auch deshalb fleissig erforscht und klargelegt zu werden, weil nicht selten daraus sich neue Hülfsmittel und Erweiterungen für die Wissenschaft ergeben.

Obwohl also der hier zu behandelnde arithmetische Satz durch frühere Bemühungen, die vier von einander ganz und gar verschiedene Beweise geliefert haben*), als vollständig erledigt erscheinen könnte, kehre ich doch von Neuem zu demselben Gegenstande zurück und füge noch zwei weitere

*) Zwei sind im vierten und fünften Abschnitt der „*Arithmetische Untersuchungen*" dargelegt, der dritte in einer besonderen Abhandlung *(Comment. Soc. Gotting. Vol. XVI*, vgl. oben S. 457) der vierte findet sich in der Abhandlung: *Summatio quarundam serierum singularium (Comment. Recentiores, Vol. I*, vgl. oben S. 463).

Beweise hinzu, welche über diese Sache sicher neues Licht verbreiten werden. Der erstere ist zwar dem dritten in gewisser Weise verwandt, weil er von demselben Hülfssatz ausgeht; später aber verfolgt er einen verschiedenen Weg, so dass er mit Recht als ein neuer Beweis gelten kann, der jenem dritten an Kürze wenn nicht überlegen sein, doch wenigstens nicht nachstehen dürfte. Der sechste Beweis aber beruht auf einem völlig verschiedenen höchst subtilen Prinzip und giebt ein neues Beispiel für den wunderbaren Zusammenhang zwischen arithmetischen Wahrheiten, die auf den ersten Anblick sehr weit von einander entfernt liegen. Diesen beiden Beweisen fügen wir einen neuen sehr einfachen Algorithmus bei, um zu entscheiden, ob eine gegebene ganze Zahl quadratischer Rest oder Nichtrest einer gegebenen Primzahl sei.

Noch ein anderer Grund war vorhanden, welcher mich die schon neun Jahre vorher versprochenen neuen Beweise erst jetzt veröffentlichen liess. Als ich nämlich vom Jahre 1805 ab die Theorie der kubischen und biquadratischen Reste, einen bei weitem schwierigeren Gegenstand, zu durchforschen begonnen hatte, ist mir beinahe dasselbe Geschick widerfahren, wie einst in der Theorie der quadratischen Reste. Ohne Weiteres nämlich wurden diejenigen Sätze, welche diese Fragen völlig erledigen und in denen eine wunderbare Analogie mit den auf die quadratischen Reste bezüglichen Sätzen vorherrscht, durch Induction gefunden, sobald sie nur auf dem geeigneten Wege gesucht wurden, dagegen blieben alle Versuche, zu allseitig vollkommenen Beweisen derselben zu gelangen, lange Zeit hindurch vergeblich. Dies gerade war der Antrieb, dass ich mich so sehr bemühte, den bereits bekannten Beweisen über die quadratischen Reste andere und andere hinzuzufügen, in der Hoffnung, dass von den vielen verschiedenen Methoden die eine oder andere etwas zur Beleuchtung des verwandten Gegenstandes beitragen könnte. Diese Hoffnung war keineswegs eitel, und die unermüdliche Arbeit wurde endlich von glücklichem Erfolge gekrönt. In Kurzem werde ich die Früchte meiner Studien zu veröffentlichen im Stande sein; bevor ich aber an dieses schwierige Werk herangehe, habe ich beschlossen, noch einmal zur Theorie der quadratischen Reste zurückzukehren, alles, was darüber noch zu sagen ist, zu erledigen und so diesem Teile der höheren Arithmetik gewissermassen Lebewohl zu sagen.

Fünfter Beweis des Fundamentaltheorems in der Theorie der quadratischen Reste.

1.

In der Einleitung schon haben wir gesagt, dass der fünfte und der dritte Beweis von demselben Hülfssatze ausgehen, den wir hier der Bequemlichkeit wegen in den der gegenwärtigen Untersuchung angemessenen Bezeichnungen wiederholen wollen.

Hülfssatz. Es sei m eine (positive ungerade) Primzahl, M eine ganze durch m nicht teilbare Zahl; man nehme die kleinsten positiven Reste der Zahlen

$$M, 2M, 3M, 4M, \ldots, \tfrac{1}{2}(m-1)M$$

nach dem Modul m, welche teils kleiner teils grösser als $\frac{1}{2}m$ sein werden, und es sei die Anzahl der letzteren gleich n. Dann ist M quadratischer Rest oder Nichtrest von m, je nachdem n gerade oder ungerade ist.

Beweis. Sind $a, b, c, d, \ldots$ diejenigen von jenen Resten, welche kleiner sind als $\frac{1}{2}m$, $a', b', c', d', \ldots$ aber die übrigen, welche grösser sind als $\frac{1}{2}m$, so werden die Complemente der letzteren zu m, nämlich $m-a'$, $m-b'$, $m-c'$, $m-d'$, $\ldots$, offenbar sämtlich kleiner als $\frac{1}{2}m$ und sowohl unter sich als von den Resten $a, b, c, d, \ldots$ verschieden sein, so dass sie mit diesen zusammengenommen, wenn auch in anderer Reihenfolge, identisch sein werden mit den sämtlichen Zahlen $1, 2, 3, 4, \ldots, \frac{1}{2}(m-1)$. Setzt man daher das Product

$$1 \cdot 2 \cdot 3 \cdot 4 \cdots \tfrac{1}{2}(m-1) = P,$$

so wird:

$$P = abcd \cdots \times (m-a')(m-b')(m-c')(m-d') \cdots,$$

und daher:

$$(-1)^n P = abcd \cdots \times (a'-m)(b'-m)(c'-m)(d'-m) \cdots$$

Ferner wird nach dem Modul m:

$$PM^{\frac{1}{2}(m-1)} \equiv abcd \cdots \times a'b'c'd' \cdots \equiv abcd \cdots \times (a'-m)(b'-m)(c'-m)(d'-m) \cdots,$$

und daher:

$$PM^{\frac{1}{2}(m-1)} \equiv P(-1)^n.$$

Hiernach ist $M^{\frac{1}{2}(m-1)} \equiv \pm 1$, wo das obere oder untere Zeichen zu nehmen ist, je nachdem n gerade oder ungerade ist, und hieraus ergiebt sich mit Hülfe des in den „*Arithmetischen Untersuchungen*" Artikel 106 (vgl. S. 73) bewiesenen Satzes die Richtigkeit unseres Hülfssatzes von selbst.

2.

Satz. Sind m, M ganze positive ungerade zu einander prime Zahlen, ist ferner n die Anzahl derjenigen unter den kleinsten positiven Resten der Zahlen

$$M, 2M, 3M, \ldots, \tfrac{1}{2}(m-1)M$$

nach dem Modul m, welche grösser als $\frac{1}{2}m$ sind, und ebenso N die Anzahl derjenigen unter den kleinsten positiven Resten der Zahlen

$$m, 2m, 3m, \ldots, \tfrac{1}{2}(M-1)m$$

nach dem Modul M, welche grösser als $\frac{1}{2}M$ sind, so sind die drei Zahlen n, N, $\frac{1}{4}(m-1)(M-1)$ entweder sämtlich gleichzeitig gerade oder eine von ihnen ist gerade und die beiden andern ungerade.

Beweis. Wir bezeichnen

mit f den Complex der Zahlen $1, 2, 3, \ldots, \frac{1}{2}(m-1)$,
mit f' den Complex der Zahlen $m-1, m-2, m-3, \ldots, \frac{1}{2}(m+1)$,
mit F den Complex der Zahlen $1, 2, 3, \ldots, \frac{1}{2}(M-1)$,
mit F' den Complex der Zahlen $M-1, M-2, M-3, \ldots, \frac{1}{2}(M+1)$.

Es wird daher n angeben, wie viele Zahlen Mf ihre kleinsten positiven Reste nach dem Modul m im Complexe f' haben, und ebenso wird N angeben, wie viele Zahlen mF ihre kleinsten positiven Reste nach dem Modul M in dem Complex F' haben. Endlich bezeichne

φ den Complex der Zahlen $1, 2, 3, \ldots, \frac{1}{2}(mM-1)$,
φ' den Complex der Zahlen $mM-1, mM-2, mM-3, \ldots, \frac{1}{2}(mM+1)$.

Da jede ganze durch m nicht teilbare Zahl nach dem Modul m entweder irgend einem Reste aus f oder irgend einem Reste aus f' congruent sein muss und ebenso jede ganze durch M nicht teilbare Zahl nach dem Modul M entweder irgend einem Reste aus F oder irgend einem Reste aus F' congruent ist, so lassen sich sämtliche Zahlen φ, unter denen offenbar keine durch m und M gleichzeitig teilbare Zahl vorkommt, in folgender Weise in acht Klassen verteilen:

I. In der ersten Klasse befinden sich die Zahlen, welche nach dem Modul m irgend einer Zahl aus f, nach dem Modul M aber irgend einer Zahl aus F congruent sind. Die Anzahl dieser Zahlen bezeichnen wir mit α.

II. Die zweite Klasse enthält die Zahlen, welche nach den Moduln m, M respective Zahlen aus f, F' congruent sind. Die Anzahl dieser setzen wir gleich β.

III. Die dritte Klasse enthält die Zahlen, welche nach den Moduln m, M respective Zahlen aus f', F congruent sind. Ihre Anzahl setzen wir gleich γ.

IV. Die vierte Klasse enthält die Zahlen, welche nach den Moduln m, M respective Zahlen aus f', F' congruent sind. Ihre Anzahl sei gleich δ.

V. Die fünfte Klasse enthält die Zahlen, welche durch m teilbar, nach dem Modul M aber Resten aus F congruent sind.

VI. Die sechste Klasse enthält die Zahlen, welche durch m teilbar, nach dem Modul M aber Resten aus F' congruent sind.

VII. Die siebente Klasse enthält die Zahlen, welche durch M teilbar, nach dem Modul m aber Resten aus f congruent sind.

VIII. Die achte Klasse enthält die Zahlen, welche durch M teilbar, nach dem Modul m aber Resten aus f' congruent sind.

Offenbar umfassen die Klassen V. und VI. zusammen sämtliche Zahlen mF; die Anzahl der in VI. enthaltenen Zahlen ist aber gleich N, demnach

ist die Anzahl der in V. enthaltenen Zahlen gleich $\frac{1}{2}(M-1)-N$. Ebenso enthalten die Klassen VII. und VIII. zusammmen genommen sämtliche Zahlen Mf; in der Klasse VIII. finden sich n, in der Klasse VII. aber $\frac{1}{2}(m-1)-n$ Zahlen.

In durchaus analoger Weise zerfallen sämtliche Zahlen φ' in acht Klassen IX. bis XVI.; behalten wir bei der Verteilung derselben dieselbe Reihenfolge bei, so ist leicht ersichtlich, dass die in den Klassen

IX, X, XI, XII, XIII, XIV, XV, XVI

enthaltenen Zahlen respective die Complemente zu mM von den in den Klassen

IV, III, II, I, VI, V, VIII, VII

enthaltenen Zahlen sind, so dass in der Klasse IX. sich δ Zahlen, in der Klasse X. sich γ Zahlen u. s. w. vorfinden. Nun ist klar, dass, wenn man alle Zahlen der ersten Klasse mit allen Zahlen der neunten Klasse zusammennimmt, alle Zahlen unterhalb mM erhalten werden, welche nach dem Modul m irgend einer Zahl aus f, nach dem Modul M aber irgend einer Zahl aus F congruent sind, und man sieht leicht, dass deren Anzahl gleich der Anzahl aller Combinationen der einzelnen Zahlen f mit jeder einzelnen der Zahlen F ist. Daher hat man:

$$\alpha+\delta=\tfrac{1}{4}(m-1)(M-1),$$

und aus analogem Grunde ist:

$$\beta+\gamma=\tfrac{1}{4}(m-1)(M-1).$$

Nimmt man alle Zahlen der Klassen II., IV., VI. zusammen, so erhält man offenbar sämtliche Zahlen unterhalb $\frac{1}{2}mM$, welche irgend einem Reste aus F' nach dem Modul M congruent sind. Ebendieselben Zahlen aber lassen sich auch so darstellen:

$$F',\ M+F',\ 2M+F',\ 3M+F',\ \ldots,\ \tfrac{1}{2}(m-3)M+F',$$

so dass also die Anzahl aller gleich $\frac{1}{4}(m-1)(M-1)$ wird, oder man hat:

$$\beta+\delta+N=\tfrac{1}{4}(m-1)(M-1).$$

Ebenso kann man, indem man alle Zahlen der Klassen III., IV., VIII. zusammennimmt, schliessen:

$$\gamma+\delta+n=\tfrac{1}{4}(m-1)(M-1).$$

Aus diesen vier Gleichungen erhält man die folgenden:

$$\begin{aligned}2\alpha&=\tfrac{1}{4}(m-1)(M-1)+n+N\\2\beta&=\tfrac{1}{4}(m-1)(M-1)+n-N\\2\gamma&=\tfrac{1}{4}(m-1)(M-1)-n+N\\2\delta&=\tfrac{1}{4}(m-1)(M-1)-n-N,\end{aligned}$$

deren jede die Richtigkeit des Satzes beweist.

3.

Wenn wir nun annehmen, dass m und M Primzahlen sind, so wird aus der Verbindung des vorhergehenden Satzes mit dem Hülfsatz im Artikel 1 sofort das Fundamentaltheorem sich ergeben. Denn es ist klar,

I. dass, sooft entweder jede der beiden Zahlen m, M oder nur eine von der Form $4k+1$ ist, die Zahl $\frac{1}{4}(m-1)(M-1)$ gerade ist und daher n und N entweder gleichzeitig gerade oder gleichzeitig ungerade sind, also entweder jede der beiden Zahlen m und M quadratischer Rest der andern oder jede von ihnen quadratischer Nichtrest der andern ist.

II. Sooft aber beide Zahlen m, M von der Form $4k+3$ sind, ist $\frac{1}{4}(m-1)(M-1)$ eine ungerade Zahl, daher eine der Zahlen n, N gerade, die andere ungerade, und somit die eine der Zahlen m, M quadratischer Rest der andern, die andere aber quadratischer Nichtrest der ersteren.

Sechster Beweis des Fundamentaltheorems in der Theorie der quadratischen Reste.

1.

Satz. Bezeichnet p eine (positive ungerade) Primzahl, n eine ganze positive durch p nicht teilbare Zahl, x eine unbestimmte Grösse, so ist die Function

$$1+x^n+x^{2n}+x^{3n}+\cdots\cdots+x^{np-n}$$

durch die Function

$$1+x+x^2+x^3+\cdots\cdots+x^{p-1}$$

teilbar.

Beweis. Nimmt man eine ganze positive Zahl g derart an, dass $gn\equiv 1$ (mod. p) wird, und setzt man $gn=1+hp$, so ist:

$$\frac{1+x^n+x^{2n}+x^{3n}+\cdots+x^{np-n}}{1+x+x^2+x^3+\cdots+x^{p-1}}=\frac{(1-x^{np})(1-x)}{(1-x^n)(1-x^p)}$$

$$=\frac{(1-x^{np})(1-x^{gn}-x+x^{hp+1})}{(1-x^n)(1-x^p)}$$

$$=\frac{1-x^{np}}{1-x^p}\cdot\frac{1-x^{gn}}{1-x^n}-\frac{x(1-x^{np})}{1-x^n}\cdot\frac{1-x^{hp}}{1-x^p},$$

und daher offenbar eine ganze Function. W. z. b. w.

Jede ganze Function von x also, welche durch $\frac{1-x^{np}}{1-x^n}$ teilbar ist, ist auch teilbar durch $\frac{1-x^p}{1-x}$.

2.

Es bezeichne α eine positive primitive Wurzel für den Modul p, d. h. es sei α eine positive ganze Zahl von der Beschaffenheit, dass die kleinsten positiven Reste der Potenzen $1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{p-2}$ nach dem Modul p ohne Rücksicht auf die Reihenfolge mit den Zahlen $1, 2, 3, 4, \ldots, p-1$ identisch werden. Bezeichnet man ferner mit $f(x)$ die Function:

$$x + x^{\alpha} + x^{\alpha^2} + x^{\alpha^3} + \cdots + x^{\alpha^{p-2}} + 1,$$

so wird offenbar $f(x) - 1 - x - x^2 - x^3 - \cdots - x^{p-1}$ durch $1 - x^p$ und daher umsomehr durch $\frac{1-x^p}{1-x} = 1 + x + x^2 + x^3 + \cdots + x^{p-1}$ teilbar sein; durch diese letztere Function wird daher auch $f(x)$ teilbar sein. Hieraus folgt aber, da x eine unbestimmte Grösse darstellt, dass auch $f(x^n)$ durch $\frac{1-x^{np}}{1-x^n}$ und somit (nach vorigem Artikel) auch durch $\frac{1-x^p}{1-x}$ teilbar ist, wenigstens sooft n eine ganze durch p nicht teilbare Zahl ist. Ist dagegen n eine ganze durch p teilbare Zahl, so werden die einzelnen um 1 verminderten Teile der Function $f(x^n)$ durch $1 - x^p$ teilbar sein; somit wird in diesem Falle auch $f(x^n) - p$ durch $1 - x^p$ und daher auch durch $\frac{1-x^p}{1-x}$ sich teilen lassen.

3.

Satz. Setzt man

$$x - x^{\alpha} + x^{\alpha^2} - x^{\alpha^3} + x^{\alpha^4} - \cdots - x^{\alpha^{p-2}} = \xi,$$

so wird $\xi^2 \mp p$ durch $\frac{1-x^p}{1-x}$ teilbar sein, wenn man das obere Zeichen nimmt, sooft p von der Form $4k+1$, das untere, sooft p von der Form $4k+3$ ist.

Beweis. Es ist leicht ersichtlich, dass von den folgenden $p-1$ Functionen

$$\begin{array}{l}
+ x\xi - x^2 + x^{\alpha+1} - x^{\alpha^2+1} + \cdots + x^{\alpha^{p-2}+1} \\
- x^{\alpha}\xi - x^{2\alpha} + x^{\alpha^2+\alpha} - x^{\alpha^3+\alpha} + \cdots + x^{\alpha^{p-1}+\alpha} \\
+ x^{\alpha^2}\xi - x^{2\alpha^2} + x^{\alpha^3+\alpha^2} - x^{\alpha^4+\alpha^2} + \cdots + x^{\alpha^{p}+\alpha^2} \\
- x^{\alpha^3}\xi - x^{2\alpha^3} + x^{\alpha^4+\alpha^3} - x^{\alpha^5+\alpha^3} + \cdots + x^{\alpha^{p+1}+\alpha^3} \\
\cdots\cdots\cdots\cdots\cdots\cdots \\
- x^{\alpha^{p-2}}\xi - x^{2\alpha^{p-2}} + x^{\alpha^{p-1}+\alpha^{p-2}} - x^{\alpha^{p}+\alpha^{p-2}} + \cdots + x^{\alpha^{2p-4}+\alpha^{p-2}}
\end{array}$$

die erste gleich 0, jede der übrigen aber durch $1-x^p$ teilbar wird. Daher ist durch $1-x^p$ auch die Summe aller teilbar, welche ist:

$$= \xi^2 - \left(f(x^2)-1\right) + \left(f(x^{\alpha+1})-1\right) - \left(f(x^{\alpha^2+1})-1\right) + \left(f(x^{\alpha^3+1})-1\right) - \cdots + \left(f(x^{\alpha^{p-2}+1})-1\right)$$

$$= \xi^2 - f(x^2) + f(x^{\alpha+1}) - f(x^{\alpha^2+1}) + f(x^{\alpha^3+1}) - \cdots + f(x^{\alpha^{p-2}+1}) = \Omega.$$

Es ist somit dieser Ausdruck Ω auch teilbar durch $\frac{1-x^p}{1-x}$. Nun ist unter den Exponenten $2,\ \alpha+1,\ \alpha^2+1,\ \alpha^3+1,\ \ldots,\ \alpha^{p-2}+1$ nur ein einziger, nämlich $\alpha^{\frac{1}{2}(p-1)}+1$, teilbar durch p, so dass nach dem vorigen Artikel die folgenden einzelnen Teile des Ausdrucks Ω

$$f(x^2),\quad f(x^{\alpha+1}),\quad f(x^{\alpha^2+1}),\quad f(x^{\alpha^3+1}),\ \ldots$$

mit Ausnahme des einen Gliedes $f(x^{\alpha^{\frac{1}{2}(p-1)}+1})$ durch $\frac{1-x^p}{1-x}$ teilbar sind. Man kann daher jene Teile weglassen, so dass durch $\frac{1-x^p}{1-x}$ auch die Function

$$\xi^2 \mp f(x^{\alpha^{\frac{1}{2}(p-1)}+1})$$

teilbar bleibt, wo das obere oder untere Zeichen gelten wird, je nachdem p von der Form $4k+1$ oder von der Form $4k+3$ ist. Und da überdies $f(x^{\alpha^{\frac{1}{2}(p-1)}+1})-p$ durch $\frac{1-x^p}{1-x}$ teilbar ist, so wird auch $\xi^2 \mp p$ durch $\frac{1-x^p}{1-x}$ teilbar sein. W. z. b. w.

Damit das doppelte Vorzeichen keine Zweideutigkeit herbeiführen könne, werden wir mit ε die Zahl $+1$ oder -1 bezeichnen, je nachdem p von der Form $4k+1$ oder $4k+3$ ist. Es wird daher $\frac{(1-x)(\xi^2-\varepsilon p)}{1-x^p}$ eine ganze Function von x sein, die wir durch Z bezeichnen wollen.

4.

Es sei q eine positive ungerade Zahl und somit $\frac{1}{2}(q-1)$ eine ganze Zahl. Dann wird also $(\xi^2)^{\frac{1}{2}(q-1)} - (\varepsilon p)^{\frac{1}{2}(q-1)}$ durch $\xi^2-\varepsilon p$ und somit auch durch $\frac{1-x^p}{1-x}$ teilbar sein. Setzen wir

$$\varepsilon^{\frac{1}{2}(q-1)} = \delta \text{ und } \xi^{q-1} - \delta p^{\frac{1}{2}(q-1)} = \frac{1-x^p}{1-x}\,Y,$$

so wird Y eine ganze Function von x und $\delta = +1$, wenn eine der Zahlen p, q oder auch jede von ihnen von der Form $4k+1$ ist, dagegen ist $\delta = -1$, sobald beide Zahlen p, q von der Form $4k+3$ sind.

5.

Nehmen wir nun an, dass q ebenfalls eine (von p verschiedene) Primzahl sei, so wird offenbar nach dem in den *„Arithmetischen Untersuchungen" Artikel 51* (vgl. oben S. 34) bewiesenen Satze

$$\xi^q - (x^q - x^{q\alpha} + x^{q\alpha^2} - x^{q\alpha^3} + \cdots - x^{q\alpha^{p-2}})$$

durch q teilbar oder von der Form qX werden, so dass X auch in Bezug auf die numerischen Coefficienten eine ganze Function von x ist (was man sich auch bei den übrigen hier vorkommenden ganzen Functionen Z, Y, W hinzuzudenken hat). Bezeichnen wir für den Modul p und die primitive Wurzel α den Index der Zahl q mit μ, d. h. ist $q \equiv \alpha^\mu$ (mod. p), so werden die Zahlen q, $q\alpha$, $q\alpha^2$, $q\alpha^3$, ..., $q\alpha^{p-2}$ nach dem Modul p respective den Zahlen α^μ, $\alpha_{\mu+}{}^1$, $\alpha^{\mu+2}$, ..., α^{p-2}, 1, α, α^2, ..., $\alpha^{\mu-1}$ congruent und daher

$$\begin{array}{l}
x^q - x^{\alpha^\mu} \\
x^{q\alpha} - x^{\alpha^{\mu+1}} \\
x^{q\alpha^2} - x^{\alpha^{\mu+2}} \\
x^{q\alpha^3} - x^{\alpha^{\mu+3}} \\
\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot \\
x^{q\alpha^{p-\mu-2}} - x^{\alpha^{p-2}} \\
x^{q\alpha^{p-\mu-1}} - x \\
x^{q\alpha^{p-\mu}} - x^{\alpha} \\
x^{q\alpha^{p-\mu+1}} - x^{\alpha^2} \\
\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot \\
x^{q\alpha^{p-2}} - x^{\alpha^{\mu-1}}
\end{array}$$

durch $1-x^p$ teilbar sein. Nimmt man diese Grössen abwechselnd positiv und negativ und summiert sie dann, so ist klar, dass die Function

$$x^q - x^{q\alpha} + x^{q\alpha^2} - x^{q\alpha^3} + \cdots - x^{q\alpha^{p-2}} \mp \xi$$

durch $1-x^p$ teilbar ist, und zwar gilt dabei das obere oder untere Zeichen, je nachdem μ gerade oder ungerade, d. h. je nachdem q quadratischer Rest oder Nichtrest von p ist. Wir setzen daher:

$$x^q - x^{q\alpha} + x^{q\alpha^2} - x^{q\alpha^3} + \cdots - x^{q\alpha^{p-2}} - \gamma\xi = (1-x^p)\,W,$$

indem wir $\gamma = +1$ oder $= -1$ annehmen, je nachdem q quadratischer Rest oder Nichtrest von p ist, und hierbei ist offenbar W eine ganze Function.

6.

Nach diesen Vorbereitungen leiten wir aus der Combination der vorhergehenden Gleichungen die folgende Gleichung her:

$$q\xi X = \varepsilon p(\delta p^{\frac{1}{2}(q-1)} - \gamma) + \frac{1-x^p}{1-x}\cdot\big(Z(\delta p^{\frac{1}{2}(q-1)} - \gamma) + Y\xi^2 - W\xi(1-x)\big).$$

Wir nehmen an, dass aus der Division der Function ξX durch

$$x^{p-1} + x^{p-2} + x^{p-3} + \cdots + x + 1$$

der Quotient U und der Rest T sich ergebe, oder dass man hat:

$$\xi X = \frac{1-x^p}{1-x}U + T,$$

so dass U, T ganze Functionen auch in Bezug auf die numerischen Coefficienten sind und zwar T sicher von niedrigerem Grade als der Divisor. Dann wird also:

$$qT - \varepsilon p(\delta p^{\frac{1}{2}(q-1)} - \gamma) = \frac{1-x^p}{1-x}[Z(\delta p^{\frac{1}{2}(q-1)} - \gamma) + Y\xi^2 - W\xi(1-x) - qU],$$

und diese Gleichung kann offenbar nur dann bestehen, wenn sowohl die linke Seite wie die rechte Seite für sich verschwinden. Es ist somit $\varepsilon p(\delta p^{\frac{1}{2}(q-1)} - \gamma)$ durch q teilbar, ebenso auch $\delta p^{\frac{1}{2}(q-1)} - \gamma$, und somit ist auch wegen $\delta^2 = 1$ die Zahl $p^{\frac{1}{2}(q-1)} - \gamma\delta$ durch q teilbar.

Wenn wir nun durch β die positiv oder negativ genommene Einheit bezeichnen, je nachdem p quadratischer Rest oder Nichtrest der Zahl q ist, so wird $p^{\frac{1}{2}(q-1)} - \beta$ durch q teilbar sein und daher auch $\beta - \gamma\delta$; dies kann aber nur geschehen, wenn $\beta = \gamma\delta$ ist. Hieraus folgt aber unmittelbar das Fundamentaltheorem. Nämlich

I. Sooft entweder jede der beiden Zahlen p, q oder nur eine von ihnen von der Form $4k+1$ und daher $\delta = +1$ ist, so wird $\beta = \gamma$ und somit ist entweder gleichzeitig q quadratischer Rest von p und p quadratischer Rest von q, oder gleichzeitig q Nichtrest von p und p Nichtrest von q.

II. Sooft beide Zahlen p, q von der Form $4k+3$ sind und daher $\delta = -1$ ist, wird $\beta = -\gamma$ und somit entweder gleichzeitig q quadratischer Rest von p und p Nichtrest von q, oder gleichzeitig q Nichtrest von p und p Rest von q. W. z. b. w.

Neuer Algorithmus, um zu entscheiden, ob eine gegebene positive ganze Zahl quadratischer Rest oder Nichtrest einer gegebenen positiven Primzahl ist.

1.

Bevor wir die neue Auflösung dieser Aufgabe darlegen, wollen wir die in den „*Arithmetischen Untersuchungen*" mitgeteilte Auflösung hier kurz

wiederholen, da sich dieselbe ziemlich einfach mit Hülfe des Fundamentaltheorems und der folgenden bekannten Sätze durchführen lässt.

I. Die Relation der Zahl a zur Zahl b (soweit jene quadratischer Rest oder Nichtrest dieser ist) ist dieselbe wie die Relation der Zahl c zu b, wenn $a \equiv c$ (mod. b) ist.

II. Ist a das Product aus den Factoren $\alpha, \beta, \gamma, \delta, \ldots$ und b eine Primzahl, so hängt die Relation von a zu b derart von der Relation dieser Factoren zu b ab, dass a quadratischer Rest oder Nichtrest von b wird, je nachdem sich unter jenen Factoren eine gerade oder ungerade Anzahl von solchen findet, welche Nichtreste von b sind. Sooft also irgend ein Factor ein Quadrat ist, hat man auf ihn bei dieser Untersuchung überhaupt nicht Rücksicht zu nehmen; wenn aber irgend ein Factor die Potenz einer ganzen Zahl mit ungeradem Exponenten ist, so kann diese ganze Zahl selbst seine Stelle vertreten.

III. Die Zahl 2 ist quadratischer Rest jeder Primzahl von der Form $8m+1$ oder $8m+7$, Nichtrest dagegen jeder Primzahl von der Form $8m+3$ oder $8m+5$.

Wenn daher eine Zahl a gegeben ist, deren Relation zu einer Primzahl b gesucht wird, so setze man für die Zahl a, falls sie grösser als b ist, vor Allem ihren kleinsten positiven Rest nach dem Modul b, und, wenn dieser Rest in seine Primfactoren zerlegt ist, so ist die Aufgabe nach Satz II auf die Ermittlung der Relation dieser einzelnen Factoren zu b zurückgeführt. Die Relation des Factors 2 (wenn derselbe nämlich einmal oder dreimal oder fünfmal u. s. w. auftritt) ist nach Satz III bekannt; die Relation der übrigen aber hängt nach dem Fundamentaltheorem von der Relation von b zu den einzelnen ab. Auf diese Weise sind also an Stelle der einen Relation der gegebenen Zahl zu der Primzahl b nunmehr einige Relationen der Zahl b zu andern ungeraden Primzahlen, welche kleiner als b sind, zu ermitteln und diese Aufgaben werden in derselben Weise auf kleinere Moduln zurückgeführt, und zwar werden offenbar diese aufeinanderfolgenden Reductionen einmal ein Ende nehmen.

2.

Um diese Auflösung durch ein **Beispiel** zu erläutern, sei die Relation der Zahl 103 zu 379 zu suchen. Da 103 bereits kleiner als 379 und selbst eine Primzahl ist, so ist sofort das Fundamentaltheorem anzuwenden, welches lehrt, dass die gesuchte Relation der Relation der Zahl 379 zu 103 entgegengesetzt ist. Letztere wiederum ist gleich der Relation der Zahl 70 zu 103, und diese hängt ab von den Relationen der Zahlen 2, 5, 7 zu 103. Die erste dieser Relationen ist nach Satz III bekannt. Die zweite hängt nach dem Fundamentaltheorem von der Relation der Zahl 103 zu 5 ab, welcher nach Satz I die Relation der Zahl 3 zu 5 gleich ist; diese wiederum hängt nach dem Fundamentaltheorem von der Relation der Zahl 5 zu 3 ab, welcher nach Satz I die nach Satz III bekannte Relation

der Zahl 2 zu 3 gleich ist. Ebenso hängt die Relation der Zahl 7 zu 103 nach dem Fundamentaltheorem von der Relation der Zahl 103 zu 7 ab, welche nach Satz I der Relation der Zahl 5 zu 7 gleich ist; diese wiederum hängt nach dem Fundamentaltheorem von der Relation der Zahl 7 zu 5 ab, welcher nach Satz I die Relation der Zahl 2 zu 5 gleich ist, und letztere ist nach Satz III bekannt. Wenn wir nun diese Analyse synthetisch darstellen wollen, so bezieht sich die Entscheidung der Frage auf vierzehn Momente, die wir hier vollständig hersetzen, damit die grössere Kürze der neuen Lösung um so deutlicher zu Tage trete.

1. Die Zahl 2 ist quadratischer Rest der Zahl 103 (Satz III).
2. Die Zahl 2 ist quadratischer Nichtrest der Zahl 3 (Satz III).
3. Die Zahl 5 ist quadratischer Nichtrest der Zahl 3 (Nach Satz I und 2).
4. Die Zahl 3 ist quadratischer Nichtrest der Zahl 5 (Fundamentaltheorem und 3).
5. Die Zahl 103 ist quadratischer Nichtrest der Zahl 5 (I und 4).
6. Die Zahl 5 ist quadratischer Nichtrest der Zahl 103 (Fundamentaltheorem und 5).
7. Die Zahl 2 ist quadratischer Nichtrest der Zahl 5 (Satz III).
8. Die Zahl 7 ist quadratischer Nichtrest der Zahl 5 (I und 7).
9. Die Zahl 5 ist quadratischer Nichtrest der Zahl 7 (Fundamentaltheorem und 8).
10. Die Zahl 103 ist quadratischer Nichtrest der Zahl 7 (I und 9).
11. Die Zahl 7 ist quadratischer Rest der Zahl 103 (Fundamentaltheorem und 10).
12. Die Zahl 70 ist quadratischer Nichtrest der Zahl 103 (II, 1.6.11).
13. Die Zahl 379 ist quadratischer Nichtrest der Zahl 103 (I und 12).
14. Die Zahl 103 ist quadratischer Rest der Zahl 103.

Im Folgenden werden wir uns der Kürze wegen des in den *Comment. Gotting. Vol. XVI* (vgl. oben S. 459) eingeführten Zeichens bedienen. Wir werden nämlich mit $[x]$ die Grösse x selbst bezeichnen, sooft x eine ganze Zahl ist, dagegen die zunächst unterhalb x gelegene ganze Zahl, sooft x eine gebrochene Grösse ist, so dass $x - [x]$ stets eine nicht negative unterhalb 1 gelegene Grösse ist.

3.

Aufgabe. Bezeichnen a, b positive zu einander prime ganze Zahlen und setzt man $[\frac{1}{2}a] = a'$, so soll man das Aggregat

$$\left[\frac{b}{a}\right] + \left[\frac{2b}{a}\right] + \left[\frac{3b}{a}\right] + \left[\frac{4b}{a}\right] + \cdots + \left[\frac{a'b}{a}\right]$$

finden.

Auflösung. Wir bezeichnen ein derartiges Aggregat der Kürze wegen mit $\varphi(a, b)$, so dass auch wird:

$$\varphi(b, a) = \left[\frac{a}{b}\right] + \left[\frac{2a}{b}\right] + \left[\frac{3a}{b}\right] + \cdots + \left[\frac{b'a}{b}\right],$$

wenn wir $[\frac{1}{2}b] = b'$ setzen. Im dritten Beweise des Fundamentaltheorems ist gezeigt worden, dass für den Fall, wo a und b ungerade Zahlen sind,

$$\varphi(a, b) + \varphi(b, a) = a'b'$$

wird, und, indem man dasselbe Verfahren einschlägt, lässt sich die Richtigkeit dieses Satzes auch leicht für den Fall nachweisen, dass die eine der beiden Zahlen a, b ungerade ist, wie wir an jener Stelle bereits erwähnt haben. Man dividiere nach Analogie des Verfahrens, nach welchem man den grössten gemeinschaftlichen Teiler zweier ganzen Zahlen sucht, die Zahl a durch b, und es sei β der Quotient und c der Rest; darauf dividiere man b durch c u. s. w., so dass man die Gleichungen erhält:

$$\begin{aligned} a &= \beta b + c \\ b &= \gamma c + d \\ c &= \delta d + e \\ d &= \varepsilon e + f \\ &\cdots\cdots \end{aligned}$$

Auf diese Weise werden wir in der Reihe der beständig abnehmenden Zahlen $b, c, d, e, f, \ldots$ endlich zur Einheit gelangen, da die Zahlen a und b nach Voraussetzung prim zu einander sind, so dass die letzte Gleichung wird:

$$k = \lambda l + 1.$$

Da man nun offenbar

$$\begin{aligned} \left[\frac{a}{b}\right] &= \left[\beta + \frac{c}{b}\right] = \beta + \left[\frac{c}{b}\right] \\ \left[\frac{2a}{b}\right] &= \left[2\beta + \frac{2c}{b}\right] = 2\beta + \left[\frac{2c}{b}\right] \\ \left[\frac{3a}{b}\right] &= \left[3\beta + \frac{3c}{b}\right] = 3\beta + \left[\frac{3c}{b}\right] \\ &\text{u. s. w.} \end{aligned}$$

hat, so ist:

$$\varphi(b, a) = \varphi(b, c) + \tfrac{1}{2}\beta(b'^2 + b'),$$

und daher:

$$\varphi(a, b) = a'b' - \tfrac{1}{2}\beta(b'^2 + b') - \varphi(b, c).$$

Aus ähnlichen Gründen wird, wenn wir $[\frac{1}{2}c] = c'$, $[\frac{1}{2}d] = d'$, $[\frac{1}{2}e] = e'$.. setzen:

$$\begin{aligned} \varphi(b, c) &= b'c' - \tfrac{1}{2}\gamma(c'^2 + c') - \varphi(c, d) \\ \varphi(c, d) &= c'd' - \tfrac{1}{2}\delta(d'^2 + d') - \varphi(d, e) \\ \varphi(d, e) &= d'e' - \tfrac{1}{2}\varepsilon(e'^2 + e') - \varphi(e, f) \\ &\cdots\cdots\cdots \\ \varphi(k, l) &= k'l' - \tfrac{1}{2}\lambda(l'^2 + l') - \varphi(l, 1). \end{aligned}$$

Hieraus erhalten wir, da offenbar $\varphi(l, 1) = 0$ ist, die Formel:

$$\begin{aligned} \varphi(a, b) &= a'b' - b'c' + c'd' - d'e' + \cdots \pm k'l' \\ &- \tfrac{1}{2}\beta(b'^2 + b') + \tfrac{1}{2}\gamma(c'^2 + c') - \tfrac{1}{2}\delta(d'^2 + d') + \tfrac{1}{2}\varepsilon(e'^2 + e') - \cdots \mp \lambda(l'^2 + l'). \end{aligned}$$

4.

Es folgt nun leicht aus dem, was in dem dritten Beweise auseinandergesetzt wurde, dass die Relation der Zahl b zu a, sooft a eine Primzahl ist, ohne Weiteres aus dem Wert des Aggregates $\varphi(a, 2b)$ erkannt wird. Je nachdem nämlich dieses Aggregat eine gerade oder ungerade Zahl ist, ist b quadratischer Rest oder Nichtrest von a. Zu demselben Zwecke aber kann man auch das Aggregat $\varphi(a, b)$ selbst anwenden, jedoch unter der Beschränkung, dass man den Fall, wo b ungerade ist, von demjenigen, wo b gerade ist, unterscheidet. Nämlich

I. Sooft b ungerade ist, ist b quadratischer Rest oder Nichtrest von a, je nachdem $\varphi(a, b)$ gerade oder ungerade ist.

II. Sooft b gerade ist, so gilt dieselbe Regel, wenn überdies a entweder von der Form $8n+1$ oder von der Form $8n+7$ ist; wenn dagegen für einen geraden Wert von b der Modul a entweder von der Form $8n+3$ oder von der Form $8n+5$ ist, so ist die entgegengesetzte Regel anzuwenden, d. h. es ist b quadratischer Rest von a, wenn $\varphi(a, b)$ ungerade, dagegen Nichtrest, wenn $\varphi(a, b)$ gerade ist.

Dies Alles ergiebt sich leicht aus Artikel 4 des dritten Beweises.

5.

Beispiel. Wenn die Relation der Zahl 103 zur Primzahl 379 gesucht wird, so hat man zur Ermittlung des Aggregats $\varphi(379, 103)$:

$a = 379$	$a' = 189$	
$b = 103$	$b' = 51$	$\beta = 3$
$c = 70$	$c' = 35$	$\gamma = 1$
$d = 33$	$d' = 16$	$\delta = 2$
$e = 4$	$e' = 2$	$\varepsilon = 8,$

demnach:

$$\varphi(379, 103) = 9639 - 1785 + 560 - 32 - 3978 + 630 - 272 + 24 = 4786,$$

so dass also 103 quadratischer Rest der Zahl 379 ist. Will man zu demselben Zwecke lieber das Aggregat $\varphi(379, 206)$ anwenden, so hat man:

379	189	
206	103	1
173	86	1
33	16	5
8	4	4,

und hieraus erhält man:

$$\varphi(379, 206) = 19467 - 8858 + 1376 - 64 - 5356 + 3741 - 680 + 40 = 9666;$$

somit ist 103 quadratischer Rest von 379.

6.

Da es zur Bestimmung der Relation der Zahl b zu a nicht nötig ist, die einzelnen Teile des Aggregats $\varphi(a, b)$ zu berechnen, sondern es ausreicht zu wissen, wie viele unter ihnen ungerade sind, so lässt sich unsere Regel auch so darstellen:

Es sei wie oben $a = \beta b + c$, $b = \gamma c + d$, $c = \delta d + e$, ..., bis man in der Reihe der Zahlen $a, b, c, d, e, \ldots$ zur Einheit kommt. Man setze $[\frac{1}{2}a] = a'$, $[\frac{1}{2}b] = b'$, $[\frac{1}{2}c] = c'$, ..., und es sei μ die Anzahl derjenigen ungeraden Zahlen in der Reihe $a', b', c', \ldots$, auf welche unmittelbar eine ungerade Zahl folgt; ferner sei ν die Anzahl derjenigen ungeraden Zahlen in der Reihe $\beta, \gamma, \delta, \ldots$, welchen in der Reihe $b', c', d', \ldots$ respective eine Zahl von der Form $4n + 1$ oder von der Form $4n + 2$ entspricht. Alsdann wird b quadratischer Rest oder Nichtrest von a sein, je nachdem $\mu + \nu$ gerade oder ungerade ist, den einzigen Fall ausgenommen, in welchem gleichzeitig b gerade und a entweder von der Form $8n + 3$ oder $8n + 5$ ist, wo dann die entgegengesetzte Regel gilt.

In unserm Beispiel bietet die Reihe $a', b', c', d', \ldots$ zwei Aufeinanderfolgen von ungeraden Zahlen dar, so dass $\mu = 2$ ist; in der Reihe $\beta, \gamma, \delta, \varepsilon$ kommen zwar zwei ungerade Zahlen vor, aber ihnen entsprechen in der Reihe b', c', d', e' Zahlen von der Form $4n + 3$, so dass also $\nu = 0$ ist. Es wird daher $\mu + \nu$ gerade, und daher ist 103 quadratischer Rest der Zahl 379.

Theorie der biquadratischen Reste.

Erste Abhandlung.

(Commentationes soc. reg. sc. Gotting. recentiores. Vol. VI. Gottingae 1828.)

1.

Die Theorie der quadratischen Reste lässt sich auf wenige den herrlichsten Kleinodien der höheren Arithmetik zuzuzählende Fundamentalsätze zurückführen, die, wie man weiss, zunächst auf inductivem Wege leicht entdeckt und darauf auf mannigfaltige Weise so bewiesen worden sind, dass nichts mehr zu wünschen übrigbleibt.

Bei weitem schwieriger aber ist die Theorie der kubischen und biquadratischen Reste. Als wir diese vom Jahre 1805 an zu durchforschen anfingen, ergaben sich zwar ausser den allerersten von selbst sich darbietenden Elementen einige specielle Sätze, welche sowohl ihrer Einfachheit wegen als auch wegen der Schwierigkeit der Beweise höchst hervorragend sind, jedoch kamen wir bald zu der Erkenntnis, dass die bisher gebräuchlichen Prinzipien der Arithmetik zur Begründung einer allgemeinen Theorie keineswegs ausreichen, dass vielmehr diese mit Notwendigkeit erforderte, das Gebiet der höheren Arithmetik gewissermassen unendlichvielmal zu vergrössern; wie dieses zu verstehen sei, wird im Verlaufe dieser Untersuchungen auf das Deutlichste zu Tage treten. Sobald wir einmal dieses neue Feld beschritten, eröffnete sich sogleich ein Zugang zur Kenntnis der einfachsten, die ganze Theorie erschöpfenden Sätze auf inductivem Wege; dagegen lagen die Beweise derselben so tief versteckt, dass sie erst nach vielen vergeblichen Versuchen endlich ans Licht gezogen werden konnten.

Indem wir jetzt zur Veröffentlichung dieser Studien schreiten, beginnen wir mit der Theorie der biquadratischen Reste, und zwar werden wir in dieser ersten Abhandlung diejenigen Untersuchungen darlegen, welche sich noch ohne eine solche Erweiterung des Feldes der Arithmetik vollständig erledigen lassen, die aber zu jener gewissermassen den Weg bahnen und zugleich für die Theorie der Kreisteilung einige neue Erweiterungen liefern.

2.

Den Begriff des **biquadratischen Restes** haben wir im Artikel 115 der *„Arithmetischen Untersuchungen“* (vgl. oben S. 79) eingeführt: Es wird nämlich eine ganze, positive oder negative Zahl a biquadratischer Rest der ganzen Zahl p genannt, wenn a nach dem Modul p einem Biquadrate congruent werden kann, und ebenso **biquadratischer Nichtrest**, wenn eine solche Congruenz nicht besteht. In allen folgenden Untersuchungen, wo nicht ausdrücklich das Gegenteil hervorgehoben wird, werden wir annehmen, dass der Modul p eine (ungerade positive) **Primzahl** und a durch p nicht teilbar sei, da alle übrigen Fälle auf diesen sehr leicht zurückgeführt werden können.

3.

Offenbar wird jeder biquadratische Rest der Zahl p auch quadratischer Rest und somit jeder quadratische Nichtrest auch biquadratischer Nichtrest derselben sein. Diesen Satz kann man auch umkehren, so oft p eine Primzahl von der Form $4n+3$ ist. Denn wenn in diesem Falle a quadratischer Rest von p ist, so setze man $a \equiv b^2$ (mod. p), wo b entweder quadratischer Rest oder Nichtrest von p sein wird. Im ersteren Falle setzen wir $b \equiv c^2$, so dass $a \equiv c^4$ ist, d. h. es wird a biquadratischer Rest von p sein; im letzteren Falle wird $-b$ quadratischer Rest von p werden (da -1 Nichtrest jeder Primzahl von der Form $4n+3$ ist), und wenn man $-b \equiv c^2$ setzt, so wird wie vorher $a \equiv c^4$ und a biquadratischer Rest von p sein. Zugleich sieht man leicht, dass es andere Lösungen der Congruenz $x^4 \equiv a$ (mod. p) ausser den beiden $x = c$ und $x = -c$ in diesem Falle nicht giebt.

Da diese auf der Hand liegenden Sätze die ganze Theorie der biquadratischen Reste für Primzahlmoduln von der Form $4n+3$ erschöpfen, so werden wir solche Moduln von unserer Untersuchung gänzlich ausschliessen oder diese auf Primzahlmoduln von der Form $4n+1$ beschränken.

4.

Ist also p eine Primzahl von der Form $4n+1$, so darf man den Satz des vorigen Artikels nicht umkehren; denn es können quadratische Reste existieren, welche nicht zugleich biquadratische Reste sind, und zwar ist dies der Fall, sooft ein quadratischer Rest dem Quadrate eines quadratischen Nichtrestes congruent ist. Denn setzt man $a \equiv b^2$, wo b quadratischer Nichtrest von p ist, so würde, wenn die Congruenz $x^4 \equiv a$ durch einen Wert $x \equiv c$ befriedigt werden könnte, $c^4 \equiv b^2$ oder das Product $(c^2 - b)(c^2 + b)$ durch p teilbar sein, wonach p entweder in dem Factor $c^2 - b$ oder in dem andern $c^2 + b$ aufgehen müsste, d. h. es würde entweder $+b$ oder $-b$ quadratischer Rest von p sein und somit müssten beide (da -1 quadratischer Rest ist) quadratische Reste von p sein, was im Widerspruch steht mit unserer Voraussetzung.

Es würden somit sämtliche durch p nicht teilbare ganze Zahlen in drei Klassen verteilt werden können, von denen die erste die biquadratischen Reste, die zweite diejenigen biquadratischen Nichtreste, welche zugleich quadratische Reste sind, die dritte die quadratischen Nichtreste enthielte. Offenbar genügt es, einer solchen Einteilung in Klassen nur die Zahlen $1, 2, 3, \ldots, p-1$ zu unterwerfen, von denen die eine Hälfte zur dritten Klasse gehören, die andere Hälfte aber sich auf die erste und zweite Klasse verteilen würde.

5.

Indessen ist es besser, **vier** Klassen festzusetzen, deren Natur in Folgendem besteht:

Es sei A der Complex aller zwischen 1 und $p-1$ (einschliesslich) gelegenen biquadratischen Reste und e ein nach Belieben gewählter quadratischer Nichtrest von p. Es sei ferner B der Complex aller kleinsten positiven aus den Producten eA nach dem Modul p sich ergebenden Reste und ebenso C, D respective der Complex der kleinsten positiven aus den Producten e^2A, e^3A nach dem Modul p entstehenden Reste. Dann sieht man leicht, dass die einzelnen Zahlen B unter einander verschieden sind, ebenso die einzelnen Zahlen C sowie die einzelnen Zahlen D, dass aber die Null unter allen diesen Zahlen nicht vorkommen kann. Ferner ist klar, dass alle in A und C enthaltenen Zahlen quadratische Reste von p, alle in B und D enthaltenen aber quadratische Nichtreste von p sind, so dass sicher die Complexe A, C keine Zahl mit dem Complex B oder D gemeinschaftlich haben können. Es kann aber auch weder A mit C noch B mit D irgend eine Zahl gemeinschaftlich haben. Denn nehmen wir an,

I. dass irgend eine Zahl aus A z. B. a auch in C vorkomme, wo sie aus dem ihr congruenten Producte e^2a', in welchem a' eine Zahl aus dem Complexe A ist, hervorgegangen sein möge, setzen wir ferner $a \equiv \alpha^4$, $a' \equiv \alpha'^4$ und nehmen wir eine ganze Zahl θ so an, dass $\theta\alpha' \equiv 1$ wird, so ist $e^2\alpha'^4 \equiv \alpha^4$ und daher, wenn man mit θ^4 multipliciert:

$$e^2 \equiv \alpha^4\theta^4,$$

d. h. e^2 ist biquadratischer Rest und daher e quadratischer Rest, was der Voraussetzung widerspricht.

II. Nimmt man ebenso an, dass irgend eine Zahl den Complexen B, D gemeinschaftlich und aus den Producten ea, e^3a' hervorgegangen sei, wo a, a' Zahlen aus dem Complexe A sind, so würde aus der Congruenz $ea \equiv e^3a'$ folgen: $a \equiv e^2a'$, und somit würde man eine Zahl haben, welche, aus dem Producte e^2a' entstanden, zu C und zugleich zu A gehören würde, was, wie wir soeben bewiesen haben, unmöglich ist.

Ferner beweist man leicht, dass alle zwischen 1 und $p-1$ incl. liegenden quadratischen Reste von p notwendig entweder in A oder in C und alle quadratischen Nichtreste von p zwischen jenen Grenzen notwendig entweder in B oder in D vorkommen müssen. Denn

I. Jeder derartige quadratische Rest, welcher zugleich biquadratischer Rest von p ist, findet sich nach Voraussetzung in A.

II. Der quadratische Rest h (welcher kleiner als p ist), welcher zugleich biquadratischer Nichtrest ist, werde $\equiv g^2$ gesetzt, wo g quadratischer Nichtrest sein wird. Man nehme eine ganze Zahl γ derart an, dass $e\gamma \equiv g$ wird, so wird γ quadratischer Rest von p sein, den wir $\equiv k^2$ setzen wollen. Dann ist:

$$h \equiv g^2 \equiv e^2\gamma^2 \equiv e^2k^4.$$

Da nun der kleinste Rest von k^4 in A vorkommt, so muss h, welches ja aus dem Producte jener Zahl und e^2 entsteht, notwendig in C enthalten sein.

III. Bezeichnet h einen zwischen den Grenzen 1 und $p-1$ liegenden quadratischen Nichtrest von p, und ermittelt man zwischen denselben Grenzen eine ganze Zahl g derart, dass man $eg \equiv h$ hat, so wird g quadratischer Rest und somit entweder in A oder in C enthalten sein; in dem ersteren Falle findet sich offenbar h unter den Zahlen B, im letzteren aber unter den Zahlen D.

Aus allem diesen folgt, dass sämtliche Zahlen $1, 2, 3, \ldots, p-1$ sich auf die vier Reihen A, B, C, D so verteilen, dass jede von ihnen in einer einzigen von diesen vorkommt, so dass jede einzelne Reihe $\frac{1}{4}(p-1)$ Zahlen enthalten muss. Bei dieser Klassifikation enthalten die Klassen A und C die in ihnen vorkommenden Zahlen wesentlich, während die Unterscheidung der Klassen B und D insofern willkürlich ist, als sie von der Wahl der Zahl e, welche selbst immer zur Klasse B zu rechnen ist, abhängt; es werden somit, wenn man an ihrer Stelle eine andere Zahl aus der Klasse D wählt, die Klassen B und D mit einander vertauscht.

6.

Da -1 quadratischer Rest von p ist, so setze man $-1 \equiv f^2 \pmod{p}$, so dass die vier Wurzeln der Congruenz $x^4 \equiv 1$ sein werden: $1, f, -1, -f$. Wenn daher a biquadratischer Rest von p ist, etwa $a \equiv \alpha^4$, so werden die vier Wurzeln der Congruenz $x^4 \equiv a$ sein: $\alpha, f\alpha, -\alpha, -f\alpha$, und man sieht leicht, dass diese unter einander incongruent sind. Hieraus geht hervor, dass, wenn man die kleinsten positiven Reste der Biquadrate 1, 16, 81, 256, ..., $(p-1)^4$ sammelt, je vier immer gleich sein werden, so dass man $\frac{1}{4}(p-1)$ verschiedene biquadratische Reste hat, welche den Complex A bilden. Sammelt man die kleinsten Reste der Biquadrate nur bis zu $(\frac{1}{2}p-\frac{1}{2})^4$, so wird jeder einzelne nur zweimal vorhanden sein.

7.

Das Product zweier biquadratischen Reste ist offenbar ein biquadratischer Rest, oder aus der Multiplikation zweier Zahlen der Klasse A entsteht immer ein Product, dessen kleinster positiver Rest zu derselben Klasse gehört. Ebenso werden die Producte aus einer Zahl aus B und einer Zahl aus D

oder aus einer Zahl aus C und einer Zahl aus C ihre kleinsten positiven Reste in A haben.

Zur Klasse B aber gehören die Reste der Producte $A \cdot B$ und $C \cdot D$, zur Klasse C die Reste der Producte $A \cdot C$, $B \cdot B$ und $D \cdot D$, endlich zur Klasse D die Reste der Producte $A \cdot D$ und $B \cdot C$.

Die Beweise sind so klar, dass es genügt, einen anzuführen. Es seien z. B. c und d Zahlen aus C und D, und es sei $c \equiv e^2 a$, $d \equiv e^3 a'$, wo a, a' Zahlen aus A bezeichnen. Dann ist $e^4 aa'$ biquadratischer Rest, d. h. der kleinste Rest dieser Zahl gehört zu A; mithin wird, da das Product $cd \equiv e \cdot e^4 aa'$ ist, der kleinste Rest desselben in B enthalten sein.

Zu gleicher Zeit kann man leicht entscheiden, zu welcher Klasse ein Product aus mehreren Factoren zu rechnen sei. Legt man nämlich der Klasse A, B, C, D respective den Character 0, 1, 2, 3 bei, so wird der Character des Products entweder dem Aggregate der Charactere der einzelnen Factoren oder dem kleinsten Reste desselben nach dem Modul 4 gleich sein.

8.

Es erschien der Mühe wert, diese elementaren Sätze ohne Zuhülfenahme der Theorie der Potenzreste zu entwickeln; benützt man aber diese, so kann man alles noch viel leichter beweisen.

Es sei g eine primitive Wurzel für den Modul p, d. h. eine Zahl von solcher Beschaffenheit, dass in der Reihe der Potenzen g, g^2, $g^3, \ldots$ keine der Potenz g^{p-1} vorhergehende der Einheit nach dem Modul p congruent wird. Dann werden die kleinsten positiven Reste der Zahlen $1, g, g^2, g^3, \ldots, g^{p-2}$, von der Reihenfolge abgesehen, mit den Zahlen $1, 2, 3, \ldots, p-1$ übereinstimmen und sich in folgender Weise in vier Klassen verteilen: Es werden gehören:

zu	die kleinsten Reste der Zahlen
A	$1, g^4, g^8, g^{12}, \ldots, g^{p-5}$
B	$g, g^5, g^9, g^{13}, \ldots, g^{p-4}$
C	$g^2, g^6, g^{10}, g^{14}, \ldots, g^{p-3}$
D	$g^3, g^7, g^{11}, g^{15}, \ldots, g^{p-2}$.

Hieraus ergeben sich sämtliche vorhergehenden Sätze ohne Weiteres.

Übrigens kann man ebenso, wie wir hier die Zahlen $1, 2, 3, \ldots, p-1$ in vier Klassen geteilt haben, deren Complexe wir mit A, B, C, D bezeichnen, jede beliebige durch p nicht teilbare ganze Zahl je nach ihrem kleinsten Reste nach dem Modul p irgend einer von diesen Klassen zuzählen.

9.

Bezeichnen wir mit f den kleinsten Rest der Potenz $g^{\frac{1}{4}(p-1)}$ nach dem Modul p, so wird offenbar, da $f^2 \equiv g^{\frac{1}{2}(p-1)} \equiv -1$ wird (*Arithm. Unters.*

Artikel 62, vgl. oben S. 42), der Buchstabe f hier dieselbe Bedeutung haben, wie im Artikel 6. Die Potenz $g^{\frac{1}{4}\lambda(p-1)}$, in welcher λ eine ganze positive Zahl bezeichnet, wird also nach dem Modul p der Zahl $1, f, -1, -f$ congruent sein, je nachdem λ respective von der Form $4m$, $4m+1$, $4m+2$, $4m+3$ ist, oder je nachdem der kleinste Rest von g^λ in A, B, C, D respective vorkommt. Hieraus erhalten wir ein sehr einfaches Kriterium, um zu entscheiden, zu welcher Klasse eine gegebene durch p nicht teilbare Zahl h zu rechnen sei; es wird nämlich h zu A, B, C oder D gehören, je nachdem die Potenz $h^{\frac{1}{4}(p-1)}$ nach dem Modul p der Zahl $1, f, -1, -f$ congruent wird.

Als Corollar folgt hieraus, dass -1 stets zur Klasse A gehört, sooft p von der Form $8n+1$, dagegen zur Klasse C, sooft p von der Form $8n+3$ ist. Ein von der Theorie der Potenzreste unabhängiger Beweis dieses Satzes lässt sich leicht nach dem, was wir im Artikel 115, III der *„Arithmetischen Untersuchungen“* (vgl. oben S. 79) dargelegt haben, führen.

10.

Da sämtliche primitiven Wurzeln für den Modul p sich ergeben aus den Resten der Potenzen g^λ, wenn man für λ sämtliche zu $p-1$ prime Zahlen nimmt, so sieht man leicht, dass jene unter die Complexe B und D gleichmässig verteilt sein werden, wenn die Basis g stets in B enthalten ist. Wenn wir nun an Stelle der Zahl g eine andere primitive Wurzel aus dem Complexe B nehmen, so wird die Klassifikation dieselbe bleiben; wenn aber eine primitive Wurzel aus dem Complexe D als Basis genommen wird, so werden sich die Klassen B und D gegenseitig vertauschen.

Wenn die Klasseneinteilung nach dem im vorigen Artikel angegebenen Kriterium vorgenommen wird, so wird die Unterscheidung zwischen den Klassen B und D davon abhängen, welche Wurzel der Congruenz $x^2 \equiv -1 \pmod{p}$ wir als characteristische Zahl f annehmen.

11.

Damit wir die subtileren Untersuchungen, zu denen wir uns jetzt wenden, um so leichter durch Beispiele erläutern können, lassen wir hier eine Construction der Klassen für alle Moduln unter 100 folgen. Für jeden einzelnen haben wir die kleinste primitive Wurzel gewählt.

$p = 5$

$g = 2,\ f = 2$

A	1
B	2
C	4
D	3

$p = 13$

$g = 2,\ f = 8$

A	1, 3, 9
B	2, 5, 6
C	4, 10, 12
D	7, 8, 11

$p = 17$

$g = 3,\ f = 13$

A	1, 4, 13, 16
B	3, 5, 12, 14
C	2, 8, 9, 15
D	6, 7, 10, 11

$p = 29$

$g = 2,\ f = 12$

A	1, 7, 16, 20, 23, 24, 25
B	2, 3, 11, 14, 17, 19, 21
C	4, 5, 6, 9, 13, 22, 28
D	8, 10, 12, 15, 18, 26, 27

$p = 37$

$g = 2,\ f = 31$

A	1, 7, 9, 10, 12, 16, 26, 33, 34
B	2, 14, 15, 18, 20, 24, 29, 31, 32
C	3, 4, 11, 21, 25, 27, 28, 30, 36
D	5, 6, 8, 13, 17, 19, 22, 23, 35

$p = 41$

$g = 6,\ f = 32$

A	1, 4, 10, 16, 18, 23, 25, 31, 37, 40
B	6, 14, 15, 17, 19, 22, 24, 26, 27, 35
C	2, 5, 8, 9, 20, 21, 32, 33, 36, 39
D	3, 7, 11, 12, 13, 28, 29, 30, 34, 38

$p = 53$

$g = 2,\ f = 30$

A	1, 10, 13, 15, 16, 24, 28, 36, 42, 44, 46, 47, 49
B	2, 3, 19, 20, 26, 30, 31, 32, 35, 39, 41, 45, 48
C	4, 6, 7, 9, 11, 17, 25, 29, 37, 38, 40, 43, 52
D	5, 8, 12, 14, 18, 21, 22, 23, 27, 33, 34, 50, 51

$p = 61$

$g = 2,\ f = 11$

A	1, 9, 12, 13, 15, 16, 20, 22, 25, 34, 42, 47, 56, 57, 58
B	2, 7, 18, 23, 24, 26, 30, 32, 33, 40, 44, 50, 51, 53, 55
C	3, 4, 5, 14, 19, 27, 36, 39, 41, 45, 46, 48, 49, 52, 60
D	6, 8, 10, 11, 17, 21, 28, 29, 31, 35, 37, 38, 43, 54, 59

$p = 73$

$g = 5,\ f = 27$

A	1, 2, 4, 8, 9, 16, 18, 32, 36, 37, 41, 55, 57, 64, 65, 69, 71, 72
B	5, 7, 10, 14, 17, 20, 28, 33, 34, 39, 40, 45, 53, 56, 59, 63, 66, 68
C	3, 6, 12, 19, 23, 24, 25, 27, 35, 38, 46, 48, 49, 50, 54, 61, 67, 70
D	11, 13, 15, 21, 22, 26, 29, 30, 31, 42, 43, 44, 47, 51, 52, 58, 60, 62

$p = 89$

$g = 3,\ f = 34$

A	1, 2, 4, 8, 11, 16, 22, 25, 32, 39, 44, 45, 50, 57, 64, 67, 73, 78, 81, 85, 87, 88
B	3, 6, 7, 12, 14, 23, 24, 28, 33, 41, 43, 46, 48, 56, 61, 65, 66, 75, 77, 82, 83, 86
C	5, 9, 10, 17, 18, 20, 21, 34, 36, 40, 42, 47, 49, 53, 55, 68, 69, 71, 72, 79, 80, 84
D	13, 15, 19, 26, 27, 29, 30, 31, 35, 37, 38, 51, 52, 54, 58, 59, 60, 62, 63, 70, 74, 76

$p = 97$

$g = 5,\ f = 22$

A	1, 4, 6, 9, 16, 22, 24, 33, 35, 36, 43, 47, 50, 54, 61, 62, 64, 73, 75, 81, 88, 91, 93, 96
B	5, 13, 14, 17, 19, 20, 21, 23, 29, 30, 41, 45, 52, 56, 67, 68, 74, 76, 77, 78, 80, 83, 84, 92
C	2, 3, 8, 11, 12, 18, 25, 27, 31, 32, 44, 48, 49, 53, 65, 66, 70, 72, 79, 85, 86, 89, 94, 95
D	7, 10, 15, 26, 28, 34, 37, 38, 39, 40, 42, 46, 51, 55, 57, 58, 59, 60, 63, 69, 71, 82, 87, 90.

12.

Da die Zahl 2 quadratischer Rest aller Primzahlen von der Form $8n+1$, dagegen quadratischer Nichtrest aller Primzahlen von der Form $8n+5$ ist, so wird für Primzahlmoduln von der ersteren Form 2 in der Klasse A oder C, für Primzahlmoduln von der letzteren Form aber in der Klasse B oder D vorkommen. Da der Unterschied zwischen den Klassen B und D kein wesentlicher ist, da er nur von der Wahl der Zahl f abhängt, so lassen wir die Moduln von der Form $8n+5$ für den Augenblick bei Seite. Unterwerfen wir aber die Moduln von der Form $8n+1$ einer inductiven Untersuchung, so finden wir, dass 2 zu A gehört für $p = 73$, 89, 113, 233, 257, 281, 337, 353, ..., dass dagegen 2 zu C gehört für $p = 17$, 41, 97, 137, 193, 241, 313, 401, 409, 433, 449, 457, ...

Da ferner für einen Primzahlmodul von der Form $8n+1$ die Zahl -1 biquadratischer Rest ist, so wird offenbar -2 stets mit $+2$ zugleich zu derselben Klasse gerechnet werden müssen.

13.

Wenn man die Beispiele des vorigen Artikels mit einander vergleicht, so scheint sich wenigstens auf den ersten Blick kein einfaches Kriterium darzubieten, nach welchem man die Moduln der ersten Art von denen der letzteren Art unterscheiden könnte. Nichtsdestoweniger giebt es zwei derartige durch Eleganz und Einfachheit ausgezeichnete Kriterien, zu deren einem die folgenden Betrachtungen führen.

Der Modul p lässt sich als Primzahl von der Form $8n+1$, und zwar nur auf eine einzige Weise, auf die Form a^2+2b^2 bringen (*Arithmetische Untersuchungen,* Artikel 182, II, vgl. oben S. 151); wir setzen dabei voraus, dass die Wurzeln a, b positiv genommen werden. Offenbar wird a ungerade, b aber gerade sein; wir setzen aber $b = 2^\lambda c$, so dass c ungerade ist. Wir bemerken nun,

I. dass, wenn man $p \equiv a^2 \pmod{c}$ hat, p quadratischer Rest von c und somit auch von den einzelnen Primfactoren ist, in welche c zerfällt; umgekehrt werden also dem Fundamentaltheorem zufolge diese einzelnen Primfactoren quadratische Reste von p sein, und daher wird auch das Product aus jenen c quadratischer Rest von p, und somit b^2 ebenso wie $-b^2$ biquadratischer Rest sein.

II. Demnach muss $-2b^2$ zu derselben Klasse gehören, in welcher die Zahl 2 vorkommt; somit wird offenbar, da $a^2 \equiv -2b^2$ ist, 2 entweder in der Klasse A oder in der Klasse C vorkommen, je nachdem a entweder quadratischer Rest oder quadratischer Nichtrest von p ist.

III. Wir nehmen nun an, dass a in seine Primfactoren zerlegt sei, von denen diejenigen, welche entweder von der Form $8m+1$ oder von der Form $8m+7$ sind, mit α, α', α'', ..., diejenigen aber, welche entweder von der Form $8m+3$ oder von der Form $8m+5$ sind, mit β, β', β'', ... bezeichnet sein mögen; die Anzahl der letzteren sei gleich μ. Da nun $p \equiv 2b^2 \pmod{a}$ ist, so wird p quadratischer Rest derjenigen Primfactoren von a sein, deren quadratischer Rest 2 ist, d. h. der Factoren α, α', α'', ..., dagegen quadratischer Nichtrest derjenigen Factoren, deren quadratischer Nichtrest 2 ist, d. h. der Factoren β, β', β'', ... Demnach werden umgekehrt dem Fundamentaltheorem zufolge die einzelnen α, α', α'', ... quadratische Reste von p, die einzelnen β, β', β'', ... aber quadratische Nichtreste von p sein. Hieraus schliessen wir also, dass das Product a quadratischer Rest oder Nichtrest von p ist, je nachdem μ gerade oder ungerade ist.

IV. Man bestätigt aber leicht, dass das Product aller α, α', α'', ... von der Form $8m+1$ oder $8m+7$ wird und dass dasselbe gilt von dem Producte aller β, β', β'', ..., wenn die Anzahl dieser gerade ist, so dass in diesem Falle notwendig auch das Product a von der Form $8m+1$ oder $8m+7$ werden muss, dass dagegen das Product aller β, β', β'', ..., sooft die Anzahl derselben ungerade ist, von der Form $8m+3$ oder $8m+5$ wird und daher in diesem Falle auch dasselbe von dem Producte a gilt.

Aus allem diesen ergiebt sich daher der elegante **Satz**:

Sooft a von der Form $8m+1$ oder $8m+7$ ist, ist die Zahl 2 in dem Complexe A enthalten; sooft dagegen a von der Form $8m+3$ oder $8m+5$ ist, findet sich die Zahl 2 in dem Complexe C.

Dies wird durch die im vorigen Artikel aufgezählten Beispiele bestätigt. Die erste Art der Moduln wird nämlich in folgender Weise zerlegt:

$$73 = 1+2\cdot 36,\quad 89=81+2\cdot 4,\quad 113=81+2\cdot 16,\quad 233=225+2\cdot 4,$$
$$257=225+2\cdot 16,\quad 281=81+2\cdot 100,\quad 337=49+2\cdot 144,\quad 353=225+2\cdot 64;$$

die zweite Art aber folgendermassen:

$$17 = 9+2\cdot 4,\quad 41 = 9+2\cdot 16,\quad 97 = 25+2\cdot 36,\quad 137 = 9+2\cdot 64,$$
$$193=121+2\cdot 36,\quad 241=169+2\cdot 36,\quad 313= 25+2\cdot 144,\quad 401= 9+2\cdot 196,$$
$$409=121+2\cdot 144,\quad 433=361+2\cdot 36,\quad 449=441+2\cdot 4,\quad 457=169+2\cdot 144.$$

14.

Da die Zerlegung der Zahl p in ein einfaches und in ein doppeltes Quadrat einen so ausgezeichneten Zusammenhang mit der Klassifikation der Zahl 2 verrät, so dürfte es der Mühe wert sein zu untersuchen, ob die Zerlegung in zwei Quadrate, die sich bekanntlich ebenfalls für die Zahl p ausführen lässt, vielleicht einen ähnlichen Erfolg verspricht. Man sieht daher hier die Zerlegungen der Zahlen p, für welche 2 gehört zu den Klassen

A	C
9 + 64	1 + 16
25 + 64	25 + 16
49 + 64	81 + 16
169 + 64	121 + 16
1 + 256	49 + 144
25 + 256	225 + 16
81 + 256	169 + 144
289 + 64	1 + 400
	9 + 400
	289 + 144
	49 + 400
	441 + 16

Vor Allem bemerken wir, dass von den beiden Quadraten, in welche p zerlegt wird, das eine, welches wir gleich a^2 setzen, ungerade, das andere, welches wir gleich b^2 setzen, gerade sein muss. Da a^2 von der Form $8n+1$ wird, so werden offenbar ungerademal geraden Werten von b Werte von p von der Form $8n+5$ entsprechen, die von unserer Untersuchung vorläufig ausgeschlossen sind, da für sie die Zahl 2 in der Klasse B oder D enthalten sein würde. Für Werte von p aber, welche von der Form $8n+1$ sind, muss b gerademal gerade sein, und wenn man unserm Inductionsschluss,

welchen das angegebene Schema vor Augen stellt, Glauben schenken darf, so wird die Zahl 2 zur Klasse A zu rechnen sein für alle Moduln, für welche b von der Form $8n$, zur Klasse C dagegen für alle Moduln, für welche b von der Form $8n+4$ ist. Dieser Satz erfordert aber eine viel tiefere Untersuchung als derjenige, welchen wir im vorigen Kapitel gefunden haben, und dem Beweise desselben müssen mehrere vorbereitende Erörterungen vorausgeschickt werden, die sich auf die Reihenfolge, in welcher die Zahlen der Complexe A, B, C, D einander folgen, beziehen.

15.

Wir bezeichnen die Anzahl der Zahlen aus dem Complexe A, auf welche unmittelbar eine Zahl aus dem Complexe A, B, C, D folgt, respective mit (00), (01), (02), (03); ebenso die Anzahl der Zahlen aus dem Complexe B, auf welche unmittelbar eine Zahl aus dem Complexe A, B, C, D folgt, respective mit (10), (11), (12), (13); und analog gebe es im Complexe C respective (20), (21), (22), (23) Zahlen, im Complexe D aber (30), (31), (32), (33) Zahlen, auf welche eine Zahl aus dem Complexe A, B, C, D folgt. Wir stellen uns die Aufgabe, diese sechzehn Anzahlen a priori zu bestimmen. Damit der Leser die allgemeinen Schlüsse um so bequemer mit den Beispielen vergleichen könne, hielten wir es für gut, die numerischen Werte der Glieder des Schemas (S)

(00), (01), (02), (03)
(10), (11), (12), (13)
(20), (21), (22), (23)
(30), (31), (32), (33)

für die einzelnen Moduln, für welche wir oben im Artikel 11 die Klasseneinteilung angegeben haben, hierherzusetzen.

$p=5$	$p=13$	$p=17$	$p=29$
0, 1, 0, 0	0, 1, 2, 0	0, 2, 1, 0	2, 3, 0, 2
0, 0, 0, 1	1, 1, 0, 1	2, 0, 1, 1	1, 1, 2, 3
0, 0, 0, 0	0, 1, 0, 1	1, 1, 1, 1	2, 1, 2, 1
0, 0, 1, 0	1, 0, 1, 1	0, 1, 1, 2	1, 2, 3, 1

$p=37$	$p=41$	$p=53$	$p=61$
2, 1, 2, 4	0, 4, 3, 2	2, 3, 6, 2	4, 3, 2, 6
2, 2, 4, 1	4, 2, 2, 2	4, 4, 2, 3	3, 3, 6, 3
2, 2, 2, 2	3, 2, 3, 2	2, 4, 2, 4	4, 3, 4, 3
2, 4, 1, 2	2, 2, 2, 4	4, 2, 3, 4	3, 6, 3, 3

$p=73$	$p=89$	$p=97$
5, 6, 4, 2	3, 8, 6, 4	2, 6, 7, 8
6, 2, 5, 5	8, 4, 5, 5	6, 8, 5, 5
4, 5, 4, 5	6, 5, 6, 5	7, 5, 7, 5
2, 5, 5, 6	4, 5, 5, 8	8, 5, 5, 6

Da sich die Moduln von der Form $8n+1$ und $8n+5$ in verschiedener Weise verhalten, müssen wir beide gesondert behandeln; wir beginnen mit den esteren.

16.

Das Zeichen (00) giebt an, auf wieviel verschiedene Arten die Gleichung $\alpha+1=\alpha'$ befriedigt werden kann, wobei α, α' unbestimmt Zahlen aus dem Complexe A bezeichnen. Da für einen Modul von der Form $8n+1$, wie wir ihn hier voraussetzen, α' und $p-\alpha'$ zu demselben Complexe gehören, so werden wir kürzer sagen, (00) drücke die Anzahl der verschiedenen Arten, der Gleichung $1+\alpha+\alpha'=p$ zu genügen, aus. Offenbar kann auch die Congruenz $1+\alpha+\alpha'\equiv 0 \pmod{p}$ die Stelle dieser Gleichung vertreten.

Ebenso giebt an:

(01) die Anzahl der Lösungen der Congruenz $1+\alpha+\beta\equiv 0 \pmod{p}$
(02) die Anzahl der Lösungen der Congruenz $1+\alpha+\gamma\equiv 0$
(03) die Anzahl der Lösungen der Congruenz $1+\alpha+\delta\equiv 0$
(11) die Anzahl der Lösungen der Congruenz $1+\beta+\beta'\equiv 0$
u. s. w.,

wenn man unbestimmt mit β und β' Zahlen aus dem Complexe B, mit γ Zahlen aus dem Complexe C, mit δ Zahlen aus dem Complexe D bezeichnet. Hieraus ergeben sich sogleich die folgenden sechs Gleichungen:

$$(01)=(10),\ (02)=(20),\ (03)=(30),\ (12)=(21),\ (13)=(31),\ (23)=(32).$$

Aus jeder gegebenen Lösung der Congruenz $1+\alpha+\beta\equiv 0$ ergiebt sich eine Lösung der Congruenz $1+\delta+\delta'\equiv 0$, wenn man für δ diejenige Zahl zwischen den Grenzen 1 und $p-1$ nimmt, für welche $\beta\delta\equiv 1$ ist (welche offenbar aus dem Complexe D sein wird), und für δ' den kleinsten positiven Rest des Productes $\alpha\delta$ (welcher ebenfalls aus dem Complexe D sein wird); ebenso kommt man offenbar von einer gegebenen Lösung der Congruenz $1+\delta+\delta'\equiv 0$ zu einer Lösung der Congruenz $1+\alpha+\beta\equiv 0$ zurück, wenn man β so annimmt, dass $\beta\delta\equiv 1$ wird, und zugleich $\alpha\equiv\beta\delta'$ setzt. Hieraus schliessen wir, dass beide Congruenzen gleichviel Lösungen besitzen, oder dass $(01)=(33)$ ist.

Auf analoge Weise erhalten wir aus der Congruenz $1+\alpha+\gamma\equiv 0$ die folgende: $\gamma'+\gamma''+1\equiv 0$, wenn wir γ' aus dem Complexe C so annehmen, dass $\gamma\gamma'\equiv 1$ und γ'' aus demselben Complexe dem Producte $\alpha\gamma'$ congruent wird. Hieraus schliessen wir leicht, dass diese beiden Congruenzen eine gleiche Anzahl von Lösungen besitzen, oder dass $(02)=(22)$ ist.

Ebenso leiten wir aus der Congruenz $1+\alpha+\delta\equiv 0$ die folgende her: $\beta+\beta'+1\equiv 0$, indem wir β, β' so annehmen, dass $\beta\delta\equiv 1$ und $\beta\alpha\equiv\beta'$ wird, und somit ist $(03)=(11)$.

Endlich leiten wir aus der Congruenz $1+\beta+\gamma\equiv 0$ auf analoge Weise sowohl die Congruenz $\delta+1+\beta'\equiv 0$ als auch die Congruenz $\gamma'+\delta'+1\equiv 0$ her und schliessen hieraus, dass $(12)=(13)=(23)$ sei.

Wir haben daher zwischen unsern sechzehn unbekannten Grössen elf Gleichungen erhalten, so dass dieselben auf fünf reduciert werden und das Schema (S) sich folgendermassen darstellen lässt:

$$\begin{matrix} h, & i, & k, & l \\ i, & l, & m, & m \\ k, & m, & k, & m \\ l, & m, & m, & i \end{matrix}$$

Man kann aber leicht drei neue Bedingungsgleichungen hinzufügen. Da nämlich auf jede Zahl des Complexes A, die letzte $p-1$ ausgenommen, eine Zahl aus irgend einem der Complexe A, B, C oder D folgen muss, so haben wir:

$$(00)+(01)+(02)+(03)=2n-1,$$

und ebenso:

$$\begin{aligned} (10)+(11)+(12)+(13)&=2n \\ (20)+(21)+(22)+(23)&=2n \\ (30)+(31)+(32)+(33)&=2n. \end{aligned}$$

In den soeben eingeführten Zeichen liefern die drei ersten Gleichungen:

$$\begin{aligned} h+i+k+l&=2n-1 \\ i+l+2m&=2n \\ k+m&=n. \end{aligned}$$

Die vierte Gleichung wird mit der zweiten identisch. Mit Hülfe dieser Gleichungen kann man drei Unbekannten eliminieren, wonach sämtliche sechzehn Unbekannte bereits auf zwei reduciert sind.

17.

Um aber die vollständige Bestimmung zu erhalten, wollen wir die Anzahl der Lösungen der Congruenz

$$1+\alpha+\beta+\gamma\equiv 0 \pmod{p},$$

wo α, β, γ unbestimmt Zahlen aus den Complexen A, B, C bezeichnen, ermitteln. Offenbar ist der Wert $\alpha=p-1$ nicht zulässig, da nicht $\beta+\gamma\equiv 0$ werden kann; substituiert man also für α der Reihe nach die übrigen Werte, so werden sich h, i, k, l respective zu A, B, C, D gehörige Werte von $1+\alpha$ ergeben. Für jeden gegebenen zu A gehörigen Wert von $1+\alpha$ aber, z. B. für $1+\alpha=\alpha°$, wird die Congruenz $\alpha°+\beta+\gamma\equiv 0$ ebenso viele Lösungen besitzen, als die Congruenz $1+\beta'+\gamma'\equiv 0$ (indem man nämlich $\beta\equiv\alpha°\beta'$, $\gamma\equiv\alpha°\gamma'$ setzt), d. h. $(12)=m$ Lösungen. Ebenso wird für jeden gegebenen zu B gehörigen Wert von $\alpha+1$, etwa für $1+\alpha=\beta°$, die Congruenz $\beta°+\beta+\gamma\equiv 0$ ebenso viele Lösungen haben, wie die Congruenz $1+\alpha'+\beta'\equiv 0$ (indem man nämlich $\beta\equiv\beta°\alpha'$, $\gamma\equiv\beta°\beta'$ setzt), d. h. $(01)=i$ Lösungen. Analog wird für jeden gegebenen zu C gehörigen

Wert von $1+\alpha$, etwa für $1+\alpha=\gamma^\circ$, die Congruenz $\gamma^\circ+\beta+\gamma\equiv 0$ auf ebenso viele verschiedene Arten gelöst werden können, wie die Congruenz $1+\delta+\alpha'\equiv 0$ (indem man nämlich $\beta\equiv\gamma^\circ\delta$, $\gamma\equiv\gamma^\circ\alpha'$ setzt), d. h. die Anzahl der Lösungen wird $(03)=l$ sein. Endlich wird für jeden gegebenen zu D gehörigen Wert von $1+\alpha$, z. B. für $1+\alpha=\delta^\circ$, die Congruenz $\delta^\circ+\beta+\gamma\equiv 0$ ebenso viele Lösungen besitzen, wie die Congruenz $1+\gamma'+\delta'\equiv 0$ (indem man $\beta\equiv\delta^\circ\gamma'$, $\gamma\equiv\delta^\circ\delta'$ setzt), d. h. $(23)=m$ Lösungen. Sammelt man also alle diese Lösungen, so ergiebt sich, dass die Congruenz $1+\alpha+\beta+\gamma\equiv 0$

$$hm+i^2+kl+lm$$

verschiedene Lösungen besitzt.

In ganz analoger Weise aber leiten wir her, dass, wenn für β der Reihe nach die einzelnen Zahlen des Complexes B gesetzt werden, die Summe $1+\beta$ respective (10), (11), (12), (13) oder i, l, m, m zu A, B, C, D gehörige Werte erhält, und dass für jeden gegebenen zu diesen Complexen gehörigen Wert von $1+\beta$ die Congruenz $1+\beta+\alpha+\gamma\equiv 0$ respective (02), (31), (20), (13) oder k, m, k, m verschiedene Lösungen besitzt, so dass die Anzahl aller Lösungen gleich

$$ik+lm+km+m^2$$

wird.

Zu demselben Werte werden wir geführt, wenn wir die Entwicklung auf die Betrachtung der Werte der Summe $1+\gamma$ gründen.

18.

Aus diesem zwiefachen Ausdrucke für dieselbe Anzahl erhalten wir die Gleichung:

$$0=hm+i^2+kl-ik-km-m^2,$$

und hieraus, indem wir h mit Hülfe der Gleichung $h=2m-k-1$ eliminieren:

$$0=(k-m)^2+i^2+kl-ik-k^2-m.$$

Die beiden letzten Gleichungen des Artikels 16 liefern aber $k=\frac{1}{2}(l+i)$, und setzt man diesen Wert ein, so geht $i^2+kl-ik-k^2$ in $\frac{1}{4}(l-i)^2$ und daher die vorstehende Gleichung, nachdem sie mit 4 multipliciert worden, in die folgende über:

$$0=4(k-m)^2+(l-i)^2-4m.$$

Hieraus folgt, da $4m=2(k+m)-2(k-m)=2n-2(k-m)$ ist:

$$2n=4(k-m)^2+2(k-m)+(l-i)^2,$$

oder:

$$8n+1=[4(k-m)+1]^2+4(l-i)^2.$$

Setzt man daher:

$$4(k-m)+1=a,\quad 2l-2i=b,$$

so erhält man:

$$p = a^2 + b^2.$$

Bekanntlich aber lässt sich p nur auf eine einzige Art in zwei Quadrate zerlegen, von denen das eine ungerade für a^2, das andere gerade für b^2 genommen werden muss, so dass a^2 und b^2 vollkommen bestimmte Zahlen sind. Aber auch a selbst wird eine ganz bestimmte Zahl sein; denn die Wurzel des Quadrats muss positiv oder negativ genommen werden, je nachdem die positive Wurzel von der Form $4M+1$ oder $4M+3$ ist. Über die Bestimmung des Vorzeichens von b werden wir sogleich sprechen.

Combiniert man nun diese neuen Gleichungen mit den drei letzten Gleichungen des Artikels 16, so werden die fünf Zahlen h, i, k, l, m durch a, b und n vollständig in folgender Weise bestimmt:

$$\begin{aligned} 8h &= 4n - 3a - 5 \\ 8i &= 4n + a - 2b - 1 \\ 8k &= 4n + a - 1 \\ 8l &= 4n + a + 2b - 1 \\ 8m &= 4n - a + 1. \end{aligned}$$

Wenn man an Stelle von n lieber den Modul p einführen will, so kann das Schema (S), nachdem die einzelnen Glieder zur Vermeidung von Brüchen mit 16 multipliciert sind, folgendermassen dargestellt werden:

$p - 6a - 11$	$p + 2a - 4b - 3$	$p + 2a - 3$	$p + 2a + 4b - 3$
$p + 2a - 4b - 3$	$p + 2a + 4b - 3$	$p - 2a + 1$	$p - 2a + 1$
$p + 2a - 3$	$p - 2a + 1$	$p + 2a - 3$	$p - 2a + 1$
$p + 2a + 4b - 3$	$p - 2a + 1$	$p - 2a + 1$	$p + 2a - 4b - 3.$

19.

Es bleibt nur noch übrig zu zeigen, wie man das der Zahl b beizulegende Vorzeichen bestimmen kann. Schon oben, Artikel 10, haben wir bemerkt, dass der Unterschied zwischen den Complexen B und D an sich kein wesentlicher ist, sondern von der Wahl der Zahl f abhängt, für welche die eine oder die andere Wurzel der Congruenz $x^2 \equiv -1$ genommen werden muss, und dass dieselben sich gegenseitig vertauschen, wenn statt der einen die andere Wurzel genommen wird. Da nun der Anblick des eben angegebenen Schemas lehrt, dass eine ähnliche Vertauschung mit einer Änderung des Zeichens von b zusammenhängt, so kann man voraussehen, dass ein Zusammenhang zwischen dem Zeichen von b und der Zahl f bestehen muss. Um diesen kennen zu lernen, bemerken wir vor allen Dingen, dass, wenn man mit μ eine ganze nicht negative Zahl bezeichnet und für z alle Zahlen $1, 2, 3, \ldots, p-1$ nimmt, nach dem Modul p entweder $\Sigma z^\mu \equiv 0$ oder $\Sigma z^\mu \equiv -1$ wird, je nachdem μ entweder durch $p-1$ nicht teilbar oder teilbar ist. Der letztere Teil des Satzes geht daraus hervor, dass man für jeden durch $p-1$ teilbaren Wert von μ $z^\mu \equiv 1$ hat; den ersteren Teil aber beweisen wir folgendermassen. Be-

zeichnet g eine primitive Wurzel, so werden sämtliche z mit den kleinsten Resten sämtlicher g^y, wenn man für y alle Zahlen 0, 1, 2, 3, ..., $p-2$ nimmt, übereinstimmen, und es wird daher $\Sigma z^\mu \equiv \Sigma g^{\mu y}$ sein. Es ist aber:

$$\Sigma g^{\mu y} = \frac{g^{\mu(p-1)} - 1}{g^\mu - 1}$$

und daher:

$$(g^\mu - 1)\,\Sigma z^\mu \equiv g^{\mu(p-1)} - 1 \equiv 0.$$

Hieraus folgt aber, da für einen durch $p-1$ nicht teilbaren Wert von μ g^μ nicht congruent 1 oder $g^\mu - 1$ durch p nicht teilbar sein kann, dass $\Sigma z^\mu \equiv 0$ ist.

Wenn man nun die Potenz $(z^4+1)^{\frac{1}{4}(p-1)}$ nach dem Binomialtheorem entwickelt, so wird nach dem vorausgeschickten Hülfssatze:

$$\Sigma(z^4+1)^{\frac{1}{4}(p-1)} \equiv -2 \pmod{p}.$$

Die kleinsten Reste aller z^4 stellen aber sämtliche Zahlen A dar, wobei jede viermal vorkommt; daher haben wir unter den kleinsten Resten von z^4+1

4(00) zu A
4(01) zu B
4(02) zu C
4(03) zu D

gehörige, und vier werden gleich 0 sein (nämlich für $z^4 \equiv p-1$). Hieraus leiten wir mit Rücksicht auf die Kriterien der Complexe A, B, C, D die Congruenz her:

$$\Sigma(z^4+1)^{\frac{1}{4}(p-1)} \equiv 4(00) + 4f\cdot(01) - 4(02) - 4f\cdot(03),$$

und daher:

$$-2 \equiv 4(00) + 4f\cdot(01) - 4(02) - 4f\cdot(03),$$

oder, indem wir für (00), (01), ... ihre im vorigen Artikel gefundenen Werte substituieren:

$$-2 \equiv -2a - 2 - 2bf.$$

Hieraus schliessen wir demnach, dass stets $a + bf \equiv 0$ oder, indem wir mit f multiplicieren,

$$b \equiv af$$

werden muss, und diese Congruenz dient, wenn die Zahl f bereits gewählt ist, zur Bestimmurg des Zeichens von b oder, wenn das Zeichen von b anderweitig vorgeschrieben ist, zur Bestimmung der Zahl f.

20.

Nachdem wir unsere Aufgabe für Moduln von der Form $8n+1$ vollständig gelöst haben, schreiten wir zu dem andern Falle, wo p von der Form $8n+5$ ist; diesen werden wir um so kürzer erledigen können, da sämtliche Schlüsse nur wenig von den vorstehenden verschieden sind.

Da für einen solchen Modul -1 zur Klasse C gehört, so sind die Complemente der Zahlen der Complexe A, B, C, D zur Summe p respective in den Klassen C, D, A, B enthalten. Hieraus folgt leicht,

dass das Zeichen:	die Anzahl der Lösungen der Congruenz bezeichnet:
(00)	$1+\alpha+\gamma\equiv 0$
(01)	$1+\alpha+\delta\equiv 0$
(02)	$1+\alpha+\alpha'\equiv 0$
(03)	$1+\alpha+\beta\equiv 0$
(10)	$1+\beta+\gamma\equiv 0$
(11)	$1+\beta+\delta\equiv 0$
(12)	$1+\beta+\alpha\equiv 0$
(13)	$1+\beta+\beta'\equiv 0$
(20)	$1+\gamma+\gamma'\equiv 0$
(21)	$1+\gamma+\delta\equiv 0$
(22)	$1+\gamma+\alpha\equiv 0$
(23)	$1+\gamma+\beta\equiv 0$
(30)	$1+\delta+\gamma\equiv 0$
(31)	$1+\delta+\delta'\equiv 0$
(32)	$1+\delta+\alpha\equiv 0$
(33)	$1+\delta+\beta\equiv 0$,

woraus man sogleich die sechs Gleichungen erhält:

$$(00)=(22),\ (01)=(32),\ (03)=(12),\ (10)=(23),\ (11)=(33),\ (21)=(30).$$

Multipliciert man die Congruenz $1+\alpha+\gamma\equiv 0$ mit der Zahl γ' aus dem Complex C, welche so gewählt ist, dass $\gamma\gamma'\equiv 1$ wird, und nimmt man für γ'' den kleinsten Rest des Products $\alpha\gamma'$, welcher offenbar auch zum Complex C zu rechnen ist, so entsteht die Congruenz $\gamma'+\gamma''+1\equiv 0$, woraus wir schliessen: $(00)=(20)$.

Auf ganz analoge Weise erhält man die Gleichungen:

$$(01)=(13),\ (03)=(31),\ (10)=(11)=(21).$$

Mit Hülfe dieser elf Gleichungen können wir unsere sechzehn Unbekannten auf fünf reducieren und das Schema (S) in folgender Form darstellen:

$$\begin{matrix} h, & i, & k, & l \\ m, & m, & l, & i \\ h, & m, & h, & m \\ m, & l, & i, & m. \end{matrix}$$

Ferner erhalten wir die Gleichungen:

$$\begin{aligned} (00)+(01)+(02)+(03) &= 2n+1 \\ (10)+(11)+(12)+(13) &= 2n+1 \\ (20)+(21)+(22)+(23) &= 2n \\ (30)+(31)+(32)+(33) &= 2n+1, \end{aligned}$$

oder, indem wir die oben eingeführten Bezeichnungen anwenden, die drei folgenden:

$$\text{(I)} \qquad \begin{aligned} h + i + k + l &= 2n + 1 \\ 2m + i + l &= 2n + 1 \\ h + m &= n, \end{aligned}$$

mit deren Hülfe somit unsere Unbekannten bereits auf zwei reduciert werden können.

Die übrigen Gleichungen leiten wir aus der Betrachtung der Anzahl der Lösungen der Congruenz $1 + \alpha + \beta + \gamma \equiv 0$ (indem wir auch hier mit α, β, γ unbestimmt Zahlen aus den Complexen A, B, C respective bezeichnen) her. Erwägt man nämlich erstens, dass $1 + \alpha$ respective h, i, k, l zu A, B, C, D gehörige Zahlen liefert, und dass man für jeden gegebenen Wert von α in diesen vier Fällen respective m, l, i, m Lösungen erhält, so ist die Anzahl aller Lösungen gleich

$$hm + il + ik + lm.$$

Zweitens wird, da $1 + \beta$ m, m, l, i zu A, B, C, D gehörige Zahlen darstellt und für jeden gegebenen Wert von β in diesen vier Fällen respective h, m, h, m Lösungen existieren, die Anzahl aller Lösungen gleich

$$hm + m^2 + hl + im$$

sein, woraus wir die Gleichung erhalten:

$$0 = m^2 + hl + im - il - ik - lm,$$

welche mit Hülfe der aus (I) abgeleiteten Gleichung $k = 2m - h$ übergeht in die folgende:

$$0 = m^2 + hl + hi - il - im - lm.$$

Nun erhalten wir aus den Gleichungen (I) auch $l + i = 1 + 2h$, daher:

$$\begin{aligned} 2i &= 1 + 2h + (i - l) \\ 2l &= 1 + 2h - (i - l). \end{aligned}$$

Substituiert man diese Werte in die vorige Gleichung, so ergiebt sich:

$$0 = 4m^2 - 4m - 1 - 8hm + 4h^2 + (i - l)^2.$$

Wenn wir nun hier schliesslich für $4m$ substituieren: $2(h + m) - 2(h - m)$ oder wegen der letzten Gleichung in (I) $2n - 2(h - m)$, so erhalten wir:

$$0 = 4(h - m)^2 - 2n + 2(h - m) - 1 + (i - l)^2,$$

und daher:

$$8n + 5 = [4(h - m) + 1]^2 + 4(i - l)^2.$$

Setzt man daher:

$$4(h - m) + 1 = a, \quad 2i - 2l = b,$$

so wird:

$$p = a^2 + b^2.$$

Da nun aber auch in diesem Falle p nur auf eine einzige Weise in zwei Quadrate, ein gerades und ein ungerades, zerlegt werden kann, so werden a^2 und b^2 völlig bestimmte Zahlen sein; denn offenbar muss a^2 dem ungeraden, b^2 dem geraden Quadrate gleichgesetzt werden. Ausserdem ist das Vorzeichen von a derart festzusetzen, dass $a \equiv 1 \pmod{4}$ wird, und das Vorzeichen von b so, dass man $b \equiv af \pmod{p}$ erhält, wie man durch Schlüsse, welche den im vorigen Artikel angewandten vollkommen analog sind, leicht beweist.

Dies vorausgesetzt, werden die fünf Zahlen h, i, k, l, m durch a, b und n folgendermassen bestimmt:

$$\begin{aligned} 8h &= 4n + a - 1 \\ 8i &= 4n + a + 2b + 3 \\ 8k &= 4n - 3a + 3 \\ 8l &= 4n + a - 2b + 3 \\ 8m &= 4n - a + 1, \end{aligned}$$

oder, wenn man die Ausdrücke durch p vorzieht, so verhalten sich die mit 16 multiplicierten Glieder des Schemas (S) wie folgt:

$p + 2a - 7$	$p + 2a + 4b + 1$	$p - 2a + 1$	$p + 2a - 4b + 1$
$p - 2a - 3$	$p - 2a - 3$	$p + 2a - 4b + 1$	$p + 2a + 4b + 1$
$p + 2a - 7$	$p - 2a - 3$	$p + 2a - 7$	$p - 2a - 3$
$p - 2a - 3$	$p + 2a - 4b + 1$	$p + 2a + 4b + 1$	$p - 2a - 3.$

21.

Nachdem wir unsere Aufgabe gelöst haben, kehren wir zur Hauptuntersuchung zurück, indem wir jetzt die vollständige Bestimmung des Complexes, zu welchem die Zahl 2 gehört, in Angriff nehmen.

I. Ist p von der Form $8n + 1$, so steht bereits fest, dass die Zahl 2 entweder in dem Complexe A oder in dem Complexe C vorkommt. Im ersteren Falle sieht man leicht, dass auch die Zahlen $\frac{1}{2}(p-1)$, $\frac{1}{2}(p+1)$ zu A gehören, während sie im letzteren zu C gehören. Erwägen wir nun, dass, wenn α und $\alpha + 1$ benachbarte Zahlen des Complexes A sind, auch $p - \alpha - 1$, $p - \alpha$ solche Zahlen sind, oder was dasselbe ist, dass von derartigen Zahlen des Complexes A, auf welche eine Zahl aus demselben Complexe folgt, stets je zwei associiert sind, nämlich α und $p - 1 - \alpha$, so wird die Anzahl solcher Zahlen, d. i. (00), immer gerade sein, falls nicht eine sich selbst associierte Zahl existiert, d. h. falls nicht $\frac{1}{2}(p-1)$ zu A gehört, in welchem Falle jene Anzahl ungerade ist. Hieraus schliessen wir, dass (00) ungerade ist, sooft 2 zum Complexe A, dagegen gerade, sooft 2 zum Complexe C gehört. Wir haben aber:

$$16\,(00) = a^2 + b^2 - 6a - 11,$$

oder, wenn wir $a = 4q + 1$, $b = r$ setzen (vgl. Artikel 14):

$$(00) = q^2 - q + r^2 - 1.$$

Da nun offenbar $q^2 - q$ stets gerade ist, so wird (00) ungerade oder gerade sein, je nachdem r gerade oder ungerade ist, und daher wird die Zahl 2 zum Complexe A oder zum Complexe C gehören, je nachdem b entweder von der Form $8m$ oder von der Form $8m + 4$ ist. Dies ist gerade der Satz, den wir im Artikel 14 durch Induction gefunden hatten.

II. Aber auch den andern Fall, wo p von der Form $8n + 5$ ist, können wir ebenso vollständig erledigen. Die Zahl 2 gehört hier entweder zu B oder zu D, und man sieht leicht, dass im ersteren Falle $\frac{1}{2}(p-1)$ zu B, $\frac{1}{2}(p+1)$ zu D, im letzteren Falle aber $\frac{1}{2}(p-1)$ zu D, $\frac{1}{2}(p+1)$ zu B gehört. Man erwäge nun, dass, wenn β eine solche Zahl aus B ist, auf welche eine Zahl aus D folgt, auch die Zahl $p - \beta - 1$ aus B und die Zahl $p - \beta$ aus D sein wird, d. h. dass stets je zwei associierte Zahlen von jener Eigenschaft vorhanden sind. Es wird daher die Anzahl jener, d. i. (13) gerade, den einen Fall ausgenommen, in welchem eine von ihnen sich selbst associiert ist, d. h. wo $\frac{1}{2}(p-1)$ zu B, $\frac{1}{2}(p+1)$ zu D gehört; alsdann wird nämlich (13) ungerade sein. Hieraus schliessen wir, dass (13) gerade ist, sooft 2 zu D, dagegen ungerade, sooft 2 zu B gehört. Wir haben aber:

$$16\,(13) = a^2 + b^2 + 2a + 4b + 1,$$

oder, wenn wir $a = 4q + 1$, $b = 4r + 2$ setzen:

$$(13) = q^2 + q + r^2 + 2r + 1.$$

Es wird daher (13) ungerade sein, wenn r gerade ist; dagegen wird (13) gerade sein, wenn r ungerade ist. Hieraus schliessen wir, dass 2 zu B gehört, sooft b von der Form $8m + 2$, dagegen zu D, sooft b von der Form $8m + 6$ ist.

Das **Resultat** dieser Untersuchungen lässt sich folgendermassen aussprechen:

Die Zahl 2 gehört zu dem Complexe A, B, C oder D, je nachdem die Zahl $\frac{1}{2}b$ von der Form $4m$, $4m + 1$, $4m + 2$, oder $4m + 3$ ist.

22.

In den *„Arithmetischen Untersuchungen“* haben wir die allgemeine Theorie der Teilung des Kreises und der Auflösung der Gleichung $x^p - 1 = 0$ dargelegt und unter Anderem gezeigt, dass, wenn μ ein Teiler der Zahl $p - 1$ ist, die Function $\frac{x^p - 1}{x - 1}$ mit Hülfe einer Hülfsgleichung von der Ordnung μ in μ Factoren von der Ordnung $\frac{p-1}{\mu}$ zerlegt werden

kann. Ausser der allgemeinen Theorie dieser Auflösung haben wir die speciellen Fälle, wo $\mu = 2$ oder $\mu = 3$ ist, in jenem Werke in den Artikeln 356—358 gesondert betrachtet und die Hülfsgleichung *a priori* aufzustellen gelehrt, d. h. ohne die Entwicklung des Schemas der kleinsten Reste der Potenzen irgend einer primitiven Wurzel für den Modul p. Nun werden, auch ohne dass wir darauf hinweisen, aufmerksame Leser den engen Zusammenhang des nächsten Falles jener Theorie, d. h. des Falles $\mu = 4$, mit den hier in den Artikeln 15 bis 20 dargelegten Untersuchungen erkennen, mit deren Hülfe auch jener Fall ohne Schwierigkeit vollständig erledigt werden kann. Doch sparen wir uns diese Erörterung für eine andere Gelegenheit auf, und haben es daher auch vorgezogen, in der gegenwärtigen Abhandlung die Untersuchung in rein arithmetischer Form ohne irgend welche Rücksichtnahme auf die Theorie der Gleichung $x^p - 1 = 0$ durchzuführen. Dagegen wollen wir zum Schlusse noch einige andere neue rein arithmetische Sätze, welche mit dem bisher behandelten Gegenstande im engsten Zusammenhange stehen, hinzufügen.

23.

Wenn die Potenz $(x^4 + 1)^{\frac{1}{2}(p-1)}$ nach dem Binomialtheorem entwickelt wird, so werden in der Entwicklung drei Glieder vorkommen, in denen der Exponent von x durch $p - 1$ teilbar ist, nämlich:

$$x^{2(p-1)}, \quad Px^{p-1} \text{ und } 1,$$

wo P den mittleren Coefficienten

$$\frac{\frac{1}{2}(p-1) \cdot \frac{1}{2}(p-3) \cdot \frac{1}{2}(p-5) \cdots \frac{1}{4}(p+3)}{1 \cdot 2 \cdot 3 \cdots \frac{1}{4}(p-1)}$$

bezeichnet. Substituiert man also für x der Reihe nach die Zahlen $1, 2, 3, \ldots, p-1$, so erhält man nach dem Hülfssatze im Artikel 19:

$$\Sigma(x^4 + 1)^{\frac{1}{2}(p-1)} \equiv -2 - P.$$

Erwägt man aber das, was wir im Artikel 19 auseinandergesetzt haben, und ferner, dass die Zahlen der Complexe A, B, C, D, zur Potenz mit dem Exponenten $\frac{1}{2}(p-1)$ erhoben, nach dem Modul p den Zahlen $+1, -1, +1, -1$ respective congruent sind, so sieht man leicht, dass

$$\Sigma(x^4 + 1)^{\frac{1}{2}(p-1)} \equiv 4(00) - 4(01) + 4(02) - 4(03)$$

und somit nach den am Schlusse der Artikel 18 und 20 angegebenen Schematen

$$\Sigma(x^4 + 1)^{\frac{1}{2}(p-1)} \equiv -2a - 2$$

wird. Die Vergleichung dieser beiden Werte liefert einen sehr eleganten **Satz:** Man hat nämlich:

$$P \equiv 2a \text{ (mod. } p).$$

Bezeichnet man die vier Producte

$$\begin{array}{ll} 1\cdot 2\cdot 3 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \tfrac{1}{4}(p-1) \\ \tfrac{1}{4}(p+3)\cdot\tfrac{1}{4}(p+7)\cdot\tfrac{1}{4}(p+11)\ldots\ldots & \tfrac{1}{2}(p-1) \\ \tfrac{1}{2}(p+1)\cdot\tfrac{1}{2}(p+3)\cdot\tfrac{1}{2}(p+5)\ldots\ldots & \tfrac{3}{4}(p-1) \\ \tfrac{1}{4}(3p+1)\cdot\tfrac{1}{4}(3p+5)\cdot\tfrac{1}{4}(3p+9)\ldots\ldots & (p-1) \end{array}$$

respective mit q, r, s, t, so stellt sich der vorstehende Satz folgendermassen dar:

$$2a \equiv \frac{r}{q} \text{ (mod. } p).$$

Da jeder der Factoren von q sein Complement zu p in t hat, so ist $q \equiv t$ (mod. p), sooft die Anzahl der Factoren gerade ist, d. h. sooft p von der Form $8n+1$ ist, dagegen $q \equiv -t$, sooft die Anzahl der Factoren ungerade oder p von der Form $8n+5$ ist. Ebenso wird im ersteren Falle $r \equiv s$, im letzteren $r \equiv -s$. In beiden Fällen ist $qr \equiv st$, und da man bekanntlich $qrst \equiv -1$ hat, so wird $q^2r^2 \equiv -1$ und daher $qr \equiv \pm f$ (mod. p) sein. Verbindet man diese Congruenz mit dem eben gefundenen Satze, so erhält man $r^2 \equiv \pm 2af$ und daher nach den Artikeln 19 und 20:

$$2b \equiv \pm r^2 \text{ (mod. } p)^{*}).$$

Es ist sehr bemerkenswert, dass die Zerlegung der Zahl p durch ganz directe Methoden gefunden werden kann; es wird nämlich die Wurzel des ungeraden Quadrats der absolut kleinste Rest von $\frac{r}{2q}$, die Wurzel des geraden Quadrats aber der absolut kleinste Rest von $\frac{1}{2}r^2$ nach dem Modul p sein. Den Ausdruck $\frac{r}{2q}$, dessen Wert für $p=5$ gleich 1 wird, kann man für grössere Werte von p auch folgendermassen darstellen:

$$\frac{6\cdot 10\cdot 14\cdot 18\cdots\cdots(p-3)}{2\cdot\ 3\cdot\ 4\cdot\ 5\cdots\cdot\tfrac{1}{4}(p-1)}.$$

Da wir aber überdies wissen, mit welchem Vorzeichen die aus dieser Formel hervorgehende Wurzel des ungeraden Quadrats behaftet ist, nämlich mit demjenigen, für welches sie von der Form $4m+1$ wird, so ist es der Beachtung wert, dass ein ähnliches allgemeines Kriterium hinsichtlich des Vorzeichens der Wurzel des geraden Quadrats bisher nicht hat gefunden werden können. Sollte jemand ein solches finden und es uns mitteilen, so würden wir ihm grossen Dank wissen. Inzwischen hielt ich es für gut, die Werte der Zahlen a, b, f, wie sie sich für Werte von p unterhalb 200 aus den kleinsten Resten der Ausdrücke $\frac{r}{2q}$, $\frac{1}{2}r^2$, qr ergeben, hier anzufügen.

---

*) und $\left\{(a \mp b)q\right\}^2 \equiv a \equiv \left(\frac{r-qr^2}{2}\right)^2$.

p	a	b	f
5	+ 1	+ 2	2
13	— 3	— 2	5
17	+ 1	— 4	13
29	+ 5	+ 2	12
37	+ 1	— 6	31
41	+ 5	+ 4	9
53	— 7	— 2	23
61	+ 5	— 6	11
73	— 3	— 8	27
89	+ 5	— 8	34
97	+ 9	+ 4	22
101	+ 1	— 10	91
109	— 3	+ 10	33
113	— 7	+ 8	15
137	— 11	+ 4	37
149	— 7	— 10	44
157	— 11	— 6	129
173	+ 13	+ 2	80
181	+ 9	+ 10	162
193	— 7	+ 12	81
197	+ 1	— 14	183.

Theorie der biquadratischen Reste.

Zweite Abhandlung.

(Commentationes soc. reg. sc. Gotting. recentiores. Vol. VII. Gottingae 1832.)

24.

In der ersten Abhandlung ist das, was zur biquadratischen Klassifikation der Zahl $+2$ erforderlich ist, vollständig erledigt worden. Wenn wir uns nämlich alle durch den Modul p (welcher als Primzahl von der Form $4n+1$ vorausgesetzt wird) nicht teilbaren Zahlen in vier Klassen A, B, C, D verteilt denken, je nachdem die einzelnen, auf die Potenz mit dem Exponenten $\frac{1}{4}(p-1)$ erhoben, nach dem Modul p den Zahlen $+1$, $+f$, -1, $-f$, wo f eine der beiden Wurzeln der Congruenz $f^2 \equiv -1 \pmod{p}$ bezeichnet, congruent werden, so finden wir, dass die Entscheidung darüber, welchem Complexe die Zahl $+2$ zuzurechnen sei, von der Zerlegung der Zahl p in zwei Quadrate abhängt, so zwar, dass, wenn $p = a^2 + b^2$ gesetzt wird, wo a^2 das ungerade, b^2 das gerade Quadrat bezeichnet, und wenn ferner vorausgesetzt wird, dass die Zeichen von a, b derart angenommen seien, dass $a \equiv 1 \pmod{4}$, $b \equiv af \pmod{p}$ wird, die Zahl $+2$ zum Complexe A, B, C, D gehören muss, je nachdem $\frac{1}{2}b$ von der Form $4n$, $4n+1$, $4n+2$, $4n+3$ respective ist.

Hieraus ergiebt sich auch unmittelbar die zur Klassifikation der Zahl -2 dienende Regel. Da nämlich -1 zur Klasse A für einen geraden Wert von $\frac{1}{2}b$, zur Klasse C aber für einen ungeraden Wert von $\frac{1}{2}b$ gehört, so wird nach dem Satze des Artikels 7 die Zahl -2 zur Klasse A, B, C, D gehören, je nachdem $\frac{1}{2}b$ von der Form $4n$, $4n+3$, $4n+2$, $4n+1$ respective ist.

Diese Sätze lassen sich auch in folgender Weise ausdrücken:

Es gehört	$+2$	-2
zum Complexe	wenn b nach dem Modul 8 congruent wird:	
A	0	0
B	$2a$	$6a$
C	$4a$	$4a$
D	$6a$	$2a$.

Man erkennt leicht, dass die Sätze, in dieser Weise ausgesprochen, nicht mehr von der Bedingung $a \equiv 1 \pmod{4}$ abhängen, sondern auch noch gelten, wenn $a \equiv 3 \pmod{4}$ ist, wofern nur die andere Bedingung $af \equiv b$ (mod. p) gewahrt bleibt.

Ebenso leicht sieht man, dass der Inhalt dieser Sätze in eleganter Weise in eine einzige Formel zusammengezogen werden kann, nämlich:

Werden a und b positiv genommen, so ist stets:

$$b^{\frac{1}{2}ab} \equiv a^{\frac{1}{2}ab} 2^{\frac{1}{4}(p-1)} (\text{mod. } p).$$

25.

Wir wollen jetzt zusehen, inwieweit die Induction die Klassifikation der Zahl 3 ergiebt. Wird die Tafel des Artikels 11 weiter fortgesetzt (indem immer die kleinste primitive Wurzel genommen wird), so zeigt dieselbe, dass $+3$ gehört

zum Complexe

A für			B für			C für			D für		
p	a	b	p	a	b	p	a	b	p	a	b
13	-3	$+2$	17	$+1$	-4	37	$+1$	-6	5	$+1$	$+2$
109	-3	$+10$	29	$+5$	$+2$	61	$+5$	-6	41	$+5$	-4
181	$+9$	$+10$	53	-7	$+2$	73	-3	-8	149	-7	$+10$
193	-7	-12	89	$+5$	-8	97	$+9$	$+4$	173	$+13$	$+2$.
229	-15	$+2$	101	$+1$	$+10$	157	-11	-6			
277	$+9$	$+14$	113	-7	-8	241	-15	-4			
			137	-11	-4						
			197	$+1$	-14						
			233	$+13$	$+8$						
			257	$+1$	-16						
			269	$+13$	$+10$						
			281	$+5$	$+16$						
			293	$+17$	$+2$						

Auf den ersten Blick wenigstens bemerken wir keinen einfachen Zusammenhang zwischen den Werten der Zahlen a, b, welchen derselbe

Complex entspricht. Wenn wir aber erwägen, dass eine ähnliche Unterscheidung in der Theorie der quadratischen Reste sich hinsichtlich der Zahl -3 nach einer einfacheren Regel bewerkstelligen lässt als hinsichtlich der Zahl $+3$, so erhalten wir die Hoffnung auf einen ebenso glücklichen Erfolg in der Theorie der biquadratischen Reste. Wir finden aber, dass -3 gehört zum Complex

A für		
p	a	b
37	$+1$	-6
61	$+5$	-6
157	-11	-6
193	-7	-12

B für		
p	a	b
5	$+1$	$+2$
17	$+1$	-4
89	$+5$	-8
113	-7	-8
137	-11	-4
149	-7	$+10$
173	$+13$	$+2$
233	$+13$	$+8$
257	$+1$	-16
281	$+5$	$+16$

C für		
p	a	b
13	-3	$+2$
73	-3	-8
97	$+9$	$+4$
109	-3	$+10$
181	$+9$	$+10$
229	-15	$+2$
241	-15	-4
277	$+9$	$+14$

D für		
p	a	b
29	$+5$	$+2$
41	$+5$	-4
53	-7	$+2$
101	$+1$	$+10$
197	$+1$	-14
269	$+13$	$+10$
293	$+17$	$+2$,

und hierbei springt das Inductionsgesetz unmittelbar in die Augen, Es gehört nämlich -3 zum Complex

A, sooft b durch 3 teilbar oder $b \equiv 0 \pmod{3}$ ist,
B, sooft $a+b$ durch 3 teilbar oder $b \equiv 2a \pmod{3}$ ist,
C, sooft a durch 3 teilbar oder $a \equiv 0 \pmod{3}$ ist,
D, sooft $a-b$ durch 3 teilbar oder $b \equiv a \pmod{3}$ ist.

26.

Ferner finden wir, dass die Zahl $+5$ zu rechnen ist zum Complexe

A für $p = 101, 109, 149, 181, 269$
B für $p = 13, 17, 73, 97, 157, 193, 197, 233, 277, 293$
C für $p = 29, 41, 61, 89, 229, 241, 281$
D für $p = 37, 53, 113, 137, 173, 257.$

Betrachten wir die Werte der Zahlen a, b, welche den einzelnen p entsprechen, so erkennen wir hier das Gesetz ebenso leicht, wie für die Klassifikation der Zahl -3. Wir kommen nämlich auf den Complex

A, sooft $b \equiv 0 \pmod{5}$
B, sooft $b \equiv a$
C, sooft $a \equiv 0$
D, sooft $b \equiv 4a$.

Es ist augenscheinlich, dass diese Regeln sämtliche Fälle umfassen, da für $b \equiv 2a$ oder $b \equiv 3a$ (mod. 5): $a^2 + b^2 \equiv 0$ werden würde, was absurd ist, da nach Voraussetzung p eine von 5 verschiedene Primzahl ist.

27.

Ebenso ergiebt die Induction, wenn man sie auf die Zahlen -7, -11, $+13$, $+17$, -19, -23 anwendet und weit genug fortsetzt, die folgenden Regeln:

Für die Zahl -7.

A	$a \equiv 0$ oder $b \equiv 0$ (mod. 7)
B	$b \equiv 4a$ oder $b \equiv 5a$
C	$b \equiv a$ oder $b \equiv 6a$
D	$b \equiv 2a$ oder $b \equiv 3a$.

Für die Zahl -11.

A	$b \equiv 0$, $5a$ oder $6a$ (mod. 11)
B	$b \equiv a$, $3a$ oder $4a$
C	$a \equiv 0$ oder $b \equiv 2a$ oder $9a$
D	$b \equiv 7a$, $8a$ oder $10a$.

Für die Zahl $+13$.

A	$b \equiv 0$, $4a$, $9a$ (mod. 13)
B	$b \equiv 6a$, $11a$, $12a$
C	$a \equiv 0$; $b \equiv 3a$, $10a$
D	$b \equiv a$, $2a$, $7a$.

Für die Zahl $+17$.

A	$a \equiv 0$; $b \equiv 0$, a, $16a$ (mod. 17)
B	$b \equiv 2a$, $6a$, $8a$, $14a$
C	$b \equiv 5a$, $7a$, $10a$, $12a$
D	$b \equiv 3a$, $9a$, $11a$, $15a$.

Für die Zahl -19.

A	$b \equiv 0$, $2a$, $5a$, $14a$, $17a$ (mod. 19)
B	$b \equiv 3a$, $7a$, $11a$, $13a$, $18a$
C	$a \equiv 0$; $b \equiv 4a$, $9a$, $10a$, $15a$
D	$b \equiv a$, $6a$, $8a$, $12a$, $16a$.

Für die Zahl -23.

A	$a \equiv 0$; $b \equiv 0$, $7a$, $10a$, $13a$, $16a$ (mod. 23)
B	$b \equiv 2a$, $3a$, $4a$, $11a$, $15a$, $17a$
C	$b \equiv a$, $5a$, $9a$, $14a$, $18a$, $22a$
D	$b \equiv 6a$, $8a$, $12a$, $19a$, $20a$, $21a$.

28.

Die auf diese Weise durch Induction gefundenen speciellen Sätze finden sich bestätigt, wie weit man die Induction auch fortsetzen möge, und lassen eine sehr hübsche Form der Kriterien erkennen. Vergleicht man sie aber unter einander, um allgemeine Schlüsse daraus abzuleiten, so bieten sich sogleich auf den ersten Blick die folgenden Bemerkungen dar.

Die Kriterien, nach denen entschieden wird, zu welcher Klasse eine Primzahl $\pm q$ (wo das obere oder untere Zeichen zu nehmen ist, je nachdem q von der Form $4n+1$ oder von der Form $4n+3$ ist) zu rechnen ist, hängen von den Formen der Zahlen a, b ab, wenn man dieselbe in Bezug auf den Modul q mit einander vergleicht. Nämlich

I. Ist $a \equiv 0$ (mod. q), so gehört $\pm q$ zu einem bestimmten Complexe, und zwar ist derselbe A für $q = 7, 17, 23$ und C für $q = 3, 11, 13, 19$, wonach sich vermuten lässt, dass der erstere Fall allgemein stattfindet, wenn q von der Form $8n \pm 1$, der letztere aber, wenn q von der Form $8n \pm 3$ ist. Übrigens sind die Complexe B und D bereits ohne Induction ausgeschlossen für einen durch q teilbaren Wert von a, in welchem Falle $p \equiv b^2$ (mod. q) wird, d. h. in welchem Falle p quadratischer Rest von q ist und daher dem Fundamentaltheorem zufolge $\pm q$ quadratischer Rest von p sein muss.

II. Ist a durch q nicht teilbar, so hängt das Kriterium von dem Werte des Ausdrucks $\frac{b}{a}$ (mod. q) ab. Dieser Ausdruck besitzt allerdings q verschiedene Werte, nämlich die Werte $0, 1, 2, 3, \ldots, q-1$; wenn aber q von der Form $4n+1$ ist, so sind die beiden Werte des Ausdrucks $\sqrt{-1}$ (mod. q) auszuschliessen, welche offenbar nicht Werte des Ausdrucks $\frac{b}{a}$ (mod. q) sein können, da stets vorausgesetzt wird, dass $p = a^2 + b^2$ eine von q verschiedene Primzahl sei. Daher ist die Anzahl der zulässigen Werte des Ausdrucks $\frac{b}{a}$ (mod. q) gleich $q-2$ für $q \equiv 1$ (mod. 4), während sie gleich q bleibt für $q \equiv 3$ (mod. 4).

Nun zerfallen diese Werte in vier Klassen, nämlich so, dass die einen, welche unbestimmt mit α zu bezeichnen sind, dem Complexe A, andere mit β zu bezeichnende dem Complexe B, andere, γ genannt, dem Complexe C, endlich die übrigen, mit δ bezeichnet, dem Complexe D entsprechen, in der Weise nämlich, dass $\pm q$ zum Complexe A, B, C, D zu rechnen ist, je nachdem man $b \equiv \alpha a$, $b \equiv \beta a$, $b \equiv \gamma a$, $b \equiv \delta a$ (mod. q) hat.

Das Gesetz dieser Verteilung aber scheint ziemlich versteckt zu liegen, obwohl sich einige allgemeine Bemerkungen unmittelbar machen lassen. Die Anzahl in drei Klassen ist dieselbe, nämlich gleich $\frac{1}{4}(q-1)$ oder $\frac{1}{4}(q+1)$, während sie in der einen (und zwar in derjenigen, welche dem Complexe mit dem Kriterium $a \equiv 0$ entspricht) um Eins kleiner ist, so dass die Anzahl aller verschiedenen Kriterien hinsichtlich der einzelnen Complexe dieselbe ist, nämlich gleich $\frac{1}{4}(q-1)$ oder $\frac{1}{4}(q+1)$. Ferner bemerken wir,

dass 0 stets in der ersten Klasse (unter α) vorkommt, sowie dass die Complemente der Zahlen α, β, γ, δ zu q, nämlich $q-\alpha$, $q-\beta$, $q-\gamma$, $q-\delta$ respective in der ersten, vierten, dritten, zweiten Klasse enthalten sind. Endlich sehen wir, dass die Werte der Ausdrücke $\frac{1}{\alpha}$, $\frac{1}{\beta}$, $\frac{1}{\gamma}$, $\frac{1}{\delta}$ (mod. q) zur ersten, vierten, dritten, zweiten Klasse gehören, wenn das Kriterium $a\equiv 0$ dem Complexe A entspricht, dagegen zur dritten, zweiten, ersten, vierten Klasse respective, wenn das Kriterium $a\equiv 0$ sich auf den Complex C bezieht. Hierauf aber ist so ziemlich alles, was sich durch Induction erreichen lässt, beschränkt, wenn wir uns nicht anmassen wollen, das, was unten aus natürlichen Quellen abgeleitet werden wird, hier vorausgesehen zu haben.

29.

Bevor wir weiter gehen, wollen wir bemerken, dass die Kriterien für Primzahlen (positiv genommen, wenn sie von der Form $4n+1$, negativ, wenn sie von der Form $4n+3$ sind) zur Entscheidung für alle übrigen Zahlen ausreichen, wenn man nur den Satz des Artikels 7 und die Kriterien für -1 und ± 2 zu Hülfe nimmt. So werden z. B., wenn man die Kriterien für die Zahl $+3$ haben will, die im Artikel 25 angegebenen auf die Zahl -3 sich beziehenden Kriterien auch noch gelten für $+3$, wenn $\frac{1}{2}b$ eine gerade Zahl ist, dagegen müssen die Complexe A, B, C, D mit den Complexen C, D, A, B vertauscht werden, wenn $\frac{1}{2}b$ eine ungerade Zahl ist, so dass wir die folgenden Regeln erhalten.

$+3$ gehört

zum Complexe	wenn
A	$b\equiv 0$ (mod. 12) oder gleichzeitig $a\equiv 0$ (mod. 3) und $b\equiv 2$ (mod. 4)
B	$b\equiv 8a$ oder $10a$ (mod. 12)
C	$b\equiv 6a$ (mod. 12) oder gleichzeitig $a\equiv 0$ (mod. 3) und $b\equiv 0$ (mod. 4)
D	$b\equiv 2a$ oder $4a$ (mod. 12).

Ebenso werden die Kriterien für ± 6 aus der Verbindung der Kriterien für ∓ 2 und -3 abgeleitet, nämlich:

$+6$ gehört

zum Complexe	wenn
A	$b\equiv 0$, $2a$, $22a$ (mod. 24) oder gleichzeitig $a\equiv 0$ (mod. 3) und $b\equiv 4a$ (mod. 8)
B	$b\equiv 4a$, $6a$, $8a$ (mod. 24) oder gleichzeitig $a\equiv 0$ (mod. 3) und $b\equiv 2a$ (mod. 8)
C	$b\equiv 10a$, $12a$, $14a$ (mod. 24) oder gleichzeitig $a\equiv 0$ (mod. 3) und $b\equiv 0$ (mod. 8)
D	$b\equiv 16a$, $18a$, $20a$ (mod. 24) oder gleichzeitig $a\equiv 0$ (mod. 3) und $b\equiv 6a$ (mod. 8).

— 6 aber gehört

zum Complexe	wenn
A	$b\equiv 0,\ 10a,\ 14a \pmod{24}$ oder gleichzeitig $a\equiv 0 \pmod{3}$ und $b\equiv 4a \pmod{8}$
B	$b\equiv 4a,\ 8a,\ 18a \pmod{24}$ oder gleichzeitig $a\equiv 0 \pmod{3}$ und $b\equiv 6a \pmod{8}$
C	$b\equiv 2a,\ 12a,\ 22a \pmod{24}$ oder gleichzeitig $a\equiv 0 \pmod{3}$ und $b\equiv 0 \pmod{8}$
D	$b\equiv 6a,\ 16a,\ 20a \pmod{24}$ oder gleichzeitig $a\equiv 0 \pmod{3}$ und $b\equiv 2a \pmod{8}$.

Auf analoge Weise setzen sich die Kriterien für die Zahl + 21 aus den Kriterien für — 3 und — 7, die Kriterien für — 105 aus den Kriterien für — 1, — 3, + 5, — 7, u. s. w, zusammen.

30.

So liefert uns also die Induction eine reiche Ernte von speciellen Sätzen, welche dem Satze für die Zahl 2 verwandt sind; aber man vermisst ein gemeinschaftliches Band, man vermisst strenge Beweise, da die Methode, durch welche wir in der ersten Abhandlung die Zahl 2 erledigt haben, eine weitere Anwendung nicht gestattet. Es fehlt zwar nicht an verschiedenen Methoden, mittelst deren man die Beweise für specielle Fälle erhalten kann, besonders diejenigen, welche sich auf die Verteilung der quadratischen Reste unter die Complexe A und C beziehen; indessen halten wir uns mit diesen nicht auf, da wir eine allgemeine, alle Fälle umfassende Theorie wünschen müssen. Nachdem wir schon im Jahre 1805 über diesen Gegenstand nachzudenken begonnen hatten, kamen wir bald zu der Überzeugung, dass die natürliche Quelle einer allgemeinen Theorie in einer **Erweiterung des Feldes** der Arithmetik zu suchen sei, wie wir schon im Artikel 1 angedeutet haben.

Während nämlich die höhere Arithmetik in den bisher behandelten Fragen es nur mit ganzen reellen Zahlen zu thun hat, erscheinen die auf die biquadratischen Reste bezüglichen Sätze nur dann in ihrer ganzen Einfachheit und natürlichen Schönheit, wenn das Feld der Arithmetik auch auf die **imaginären** Zahlen erstreckt wird, so dass ohne Einschränkung die Zahlen von der Form $a+bi$ das Object derselben bilden, wo, wie gewöhnlich, i die imaginäre Grösse $\sqrt{-1}$ und a, b unbestimmt alle ganzen reellen Zahlen zwischen $-\infty$ und $+\infty$ bezeichnen. Derartige Zahlen werden wir **ganze complexe Zahlen** nennen, so zwar, dass die reellen den complexen Zahlen nicht gegenübergestellt, sondern als eine besondere Art von diesen betrachtet werden. Die gegenwärtige Abhandlung wird sowohl die elementare Lehre von den complexen Grössen als auch die ersten Anfänge der Theorie der biquadratischen Reste

enthalten, deren vollkommene Ausbildung wir uns in einer nachfolgenden Fortsetzung zur Aufgabe setzen werden.*)

31.

Vor allen Dingen schicken wir einige Benennungen voraus, deren Einführung eine grössere Kürze und Durchsichtigkeit ermöglichen wird.

Das Gebiet der complexen Zahlen $a+bi$ enthält:

I. Die reellen Zahlen, in denen $b=0$ ist, und unter diesen je nach der Beschaffenheit von a

1) die Null,
2) die positiven Zahlen,
3) die negativen Zahlen;

II. Die imaginären Zahlen, in denen b von Null verschieden ist. Hier werden wiederum unterschieden

1) imaginäre Zahlen ohne reellen Teil, d. h. solche, in denen $a=0$ ist,
2) imaginäre Zahlen mit reellem Teil, d. h. solche, in denen weder b noch a gleich Null ist.

Die ersteren kann man, wenn man will, reine imaginäre Zahlen, die andern gemischte imaginäre Zahlen nennen.

In dieser Theorie benutzen wir vier Einheiten: $+1$, -1, $+i$, $-i$, welche einfach die positive, die negative, die positiv imaginäre, die negativ imaginäre Einheit heissen sollen.

Die drei Producte aus irgend einer complexen Zahl in eine der Zahlen -1, $+i$, $-i$, werden wir die jener **associierten** Zahlen nennen. Mit Ausnahme der Null (welche sich selbst associiert ist) sind also stets je vier verschiedene Zahlen einander associiert.

Dagegen nennen wir diejenige Zahl, welche aus einer complexen Zahl durch Vertauschung von i mit $-i$ hervorgeht, die zu ihr **conjugierte** Zahl. Unter den imaginären Zahlen sind also stets je zwei verschiedene conjugiert, während die reellen Zahlen sich selbst conjugiert sind, wofern man diese Benennung auf diese Zahlen ausdehnen will.

Das Product aus einer complexen Zahl und der zu ihr conjugierten Zahl nennen wir die **Norm** einer jeden von beiden. Für eine reelle Zahl ist daher ihr Quadrat als Norm zu betrachten.

---

*) Nur nebenbei wollen wir hier wenigstens noch bemerken, dass eine derartige Erweiterung des Feldes der Theorie der biquadratischen Reste besonders angepasst ist. Die Theorie der kubischen Reste muss in ähnlicher Weise auf die Betrachtung der Zahlen von der Form $a+bh$, wo h eine imaginäre Wurzel der Gleichung $h^3-1=0$, etwa $h=-\frac{1}{2}+\sqrt{\frac{3}{4}}\cdot i$ ist, gegründet werden, und ebenso erfordert die Theorie der Reste der höheren Potenzen die Einführung anderer imaginärer Grössen.

Allgemein hat man je acht mit einander im Zusammenhang stehende Zahlen, nämlich:

$$\begin{array}{r|r} a+bi & a-bi \\ -b+ai & -b-ai \\ -a-bi & -a+bi \\ b-ai & b+ai; \end{array}$$

hierbei sehen wir zwei Quaternionen von associierten Zahlen und vier Paare von conjugierten Zahlen, und die gemeinschaftliche Norm aller ist a^2+b^2. Die acht Zahlen reducieren sich aber auf vier verschiedene, wenn entweder $a=\pm b$ oder eine der beiden Zahlen a, b gleich 0 ist.

Aus den angegebenen Definitionen ergiebt sich sogleich Folgendes:

Dem Producte zweier complexen Zahlen ist das Product aus den zu ihnen conjugierten Zahlen conjugiert.

Dasselbe gilt von dem Producte mehrerer Factoren sowie auch von den Quotienten.

Die Norm des Products aus zwei complexen Zahlen ist gleich dem Product der Normen jener Zahlen.

Dieser Satz erstreckt sich auch auf Producte aus beliebig vielen Factoren und auf Quotienten.

Die Norm jeder complexen Zahl (mit Ausnahme der Null, was wir von hier ab meistens stillschweigend hinzudenken) ist eine positive Zahl.

Ferner steht nichts im Wege, unsere Definitionen auf gebrochene oder selbst irrationale Werte von a, b auszudehnen; aber $a+bi$ soll nur dann eine **ganze complexe Zahl** genannt werden, wenn jede der beiden Zahlen a, b ganz, und nur dann eine rationale Zahl, wenn jede der beiden Zahlen a, b rational ist.

32.

Der Algorithmus der arithmetischen Operationen bezüglich der complexen Zahlen ist allgemein bekannt; die Division wird durch Einführung der Norm auf die Multiplikation zurückgeführt, da man hat:

$$\frac{a+bi}{c+di}=(a+bi)\frac{c-di}{c^2+d^2}=\frac{ac+bd}{c^2+d^2}+\frac{bc-ad}{c^2+d^2}i.$$

Die Ausziehung der Quadratwurzel geschieht mit Hülfe der Formel:

$$\sqrt{a+bi}=\pm\left(\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}}+i\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}\right),$$

wenn b eine positive Zahl, oder mit Hülfe der Formel:

$$\sqrt{a+bi}=\pm\left(\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}}-i\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}\right),$$

wenn b eine negative Zahl ist. Welchen Nutzen die Transformation der complexen Grösse $a+bi$ in $r(\cos\varphi+i\sin\varphi)$ für die Erleichterung der Rechnung bietet, damit brauchen wir uns hier nicht aufzuhalten.

33.

Eine ganze complexe Zahl, welche sich in zwei von den Einheiten verschiedene*) Factoren zerlegen lässt, nennen wir eine **zusammengesetzte** complexe Zahl; dagegen heisst eine Zahl, welche eine solche Zerlegung nicht zulässt, eine complexe **Primzahl**. Hieraus geht sogleich hervor, dass jede zusammengesetzte reelle Zahl auch eine zusammengesetzte complexe Zahl ist. Dagegen kann eine reelle Primzahl eine zusammengesetze complexe Zahl sein, und zwar wird dies gelten von der Zahl 2 und allen reellen positiven Primzahlen von der Form $4n+1$ (mit Ausnahme der Zahl 1), da man diese bekanntlich in zwei positive Quadrate zerlegen kann; z. B. wird $2=(1+i)(1-i)$, $5=(1+2i)(1-2i)$, $13=(3+2i)(3-2i)$, $17=(1+4i)(1-4i)$, u. s. w.

Dagegen sind die positiven reellen Primzahlen von der Form $4n+3$ stets auch complexe Primzahlen. Denn wenn eine solche Zahl $q=(a+bi)(\alpha+\beta i)$ wäre, so würde auch $q=(a-bi)(\alpha-\beta i)$ und daher $q^2=(a^2+b^2)(\alpha^2+\beta^2)$ sein; nun kann aber q^2 nur auf eine einzige Weise in positive Factoren, welche grösser als 1 sind, zerlegt werden, nämlich in $q\cdot q$, so dass $q=a^2+b^2=\alpha^2+\beta^2$ sein müsste. Dies ist aber absurd, da die Summe zweier Quadrate nicht von der Form $4n+3$ sein kann.

Bei den negativen reellen Zahlen gelten offenbar dieselben Benennungen wie bei den positiven und dasselbe gilt von den reinen imaginären Zahlen.

Es bleibt daher nur übrig zu zeigen, wie man bei den gemischten imaginären Zahlen die zusammengesetzten von den primen Zahlen unterscheiden kann, und dies geschieht durch den folgenden Satz.

Satz. Jede ganze gemischte imaginäre Zahl $a+bi$ ist entweder eine complexe Primzahl oder eine zusammengesetzte Zahl, je nachdem ihre Norm entweder eine reelle Primzahl oder eine zusammengesetzte Zahl ist.

Beweis. I. Da die Norm einer zusammengesetzten complexen Zahl stets eine zusammengesetzte Zahl ist, so muss offenbar eine complexe Zahl, deren Norm eine reelle Primzahl ist, notwendig eine complexe Primzahl sein. Dies ist der erste Teil des Satzes.

II. Ist aber die Norm a^2+b^2 eine zusammengesetzte Zahl, so sei p

*) oder, was dasselbe ist, in solche Factoren, deren Normen grösser als die Einheit sind.

eine reelle positive Primzahl, welche in jener aufgeht. Nun sind zwei Fälle zu unterscheiden.

1. Ist p von der Form $4n+3$, so kann bekanntlich a^2+b^2 durch p nur teilbar sein, wenn p gleichzeitig in a und b aufgeht, so dass also $a+bi$ eine zusammengesetzte Zahl sein wird.

2. Ist p nicht von der Form $4n+3$, so lässt sie sich sicher in zwei Quadrate zerlegen; wir setzen daher $p=\alpha^2+\beta^2$. Da

$$(a\alpha+b\beta)(a\alpha-b\beta)=a^2(\alpha^2+\beta^2)-\beta^2(a^2+b^2)$$

und daher durch p teilbar ist, so wird sicher p in einem der beiden Factoren $a\alpha+b\beta$, $a\alpha-b\beta$ aufgehen, und da ferner

$$(a\alpha+b\beta)^2+(a\alpha-a\beta)^2=(a\alpha-b\beta)^2+(b\alpha+a\beta)^2=(a^2+b^2)(\alpha^2+\beta^2)$$

und somit durch p^2 teilbar ist, so wird offenbar in dem ersteren Falle auch $b\alpha-a\beta$, in dem letzteren $b\alpha+a\beta$ durch p teilbar sein müssen. Daher ist in dem ersteren Falle

$$\frac{a+bi}{\alpha+\beta i}=\frac{a\alpha+b\beta}{p}+\frac{b\alpha-a\beta}{p}i,$$

in dem letzteren aber

$$\frac{a+bi}{\alpha-\beta i}=\frac{a\alpha-b\beta}{p}+\frac{b\alpha+a\beta}{p}i$$

eine ganze complexe Zahl. Da somit die gegebene Zahl entweder durch $\alpha+\beta i$ oder durch $\alpha-\beta i$ teilbar ist und die Norm des Quotienten, nämlich $\frac{a^2+b^2}{p}$, nach Voraussetzung von der Einheit verschieden ist, so folgt, dass $a+bi$ in beiden Fällen eine zusammengesetzte complexe Zahl ist. Dies ist der zweite Teil des Satzes.

34.

Es wird daher die Gesamtheit der complexen Primzahlen durch folgende vier Arten vollständig erschöpft:

1. die vier Einheiten 1, $+i$, -1, $-i$, die wir jedoch, sobald wir von Primzahlen handeln, meistens stillschweigend als ausgeschlossen betrachten werden.

2. die Zahl $1+i$ mit den drei zu ihr associierten Zahlen $-1+i$, $-1-i$, $1-i$.

3). die reellen positiven Primzahlen von der Form $4n+3$ mit den drei zu ihnen associierten Zahlen.

4). die complexen Zahlen, deren Normen reelle die Einheit übersteigende Primzahlen von der Form $4n+1$ sind, und zwar werden einer jeden gegebenen Norm dieser Art je acht complexe Primzahlen und nicht mehr entsprechen, da eine solche Norm nur auf eine einzige Weise in zwei Quadrate zerlegt werden kann.

35.

Ebenso wie die reellen ganzen Zahlen in gerade und ungerade Zahlen und jene wiederum in gerademal gerade und ungerademal gerade zerfallen, so bietet sich auch bei den complexen Zahlen ein ebenso wesentlicher Unterschied dar. Sie sind nämlich

entweder durch $1+i$ nicht teilbar, z. B. die Zahlen $a+bi$, wo die eine der Zahlen a, b ungerade, die andere gerade ist,

oder durch $1+i$ aber nicht durch 2 teilbar, wenn jede der beiden Zahlen a, b ungerade ist,

oder durch 2 teilbar, wenn jede der beiden Zahlen a, b gerade ist.

Die Zahlen der ersten Klasse können passend **ungerade**, die der zweiten Klasse **halbgerade**, die der dritten Klasse **gerade** complexe Zahlen genannt werden.

Das Product aus mehreren complexen Factoren ist stets ungerade, wenn sämtliche Factoren ungerade sind; es ist halbgerade, wenn ein Factor halbgerade, die übrigen ungerade sind; es ist aber gerade, wenn unter den Factoren entweder mindestens zwei halbgerade vorkommen oder wenigstens einer gerade ist.

Die Norm jeder ungeraden complexen Zahl ist von der Form $4n+1$; die Norm einer halbgeraden Zahl von der Form $8n+2$; endlich ist die Norm einer geraden Zahl das Product aus einer Zahl von der Form $4n+1$ und der Zahl 4 oder einer höheren Potenz von 2.

36.

Da der Zusammenhang zwischen je vier associierten complexen Zahlen dem Zusammenhang zwischen zwei entgegengesetzten reellen Zahlen (d. h. zwischen zwei Zahlen, die absolut genommen gleich, aber mit entgegengesetzten Vorzeichen behaftet sind) analog ist, und von diesen allgemein die positive gleichsam als primäre Zahl mit Recht betrachtet zu werden pflegt, so entsteht die Frage, ob eine ähnliche Unterscheidung zwischen je vier associierten complexen Zahlen festgestellt werden kann und für nützlich erachtet werden muss. Um diese Frage zu entscheiden, muss man erwägen, dass das Prinzip der Unterscheidung derart beschaffen sein muss, dass das Product zweier Zahlen, welche unter den zu ihnen associierten als primäre Zahlen gelten, immer eine primäre Zahl unter den zu ihm associierten Zahlen wird. Wir überzeugen uns aber bald, dass es ein solches Prinzip überhaupt nicht giebt, wofern nicht die Unterscheidung auf ganze Zahlen beschränkt wird; ja eine nutzbringende Unterscheidung wird sogar nur auf die ungeraden Zahlen beschränkt sein. Für diese aber kann das vorgesteckte Ziel auf doppelte Weise erreicht werden, nämlich

I. Das Product aus zwei Zahlen $a+bi$, $a'+b'i$, welche so beschaffen sind, dass a, a' von der Form $4n+1$ und b, b' gerade sind, wird dieselbe Eigenschaft besitzen, so dass also der reelle Teil $\equiv 1 \pmod{4}$ und der

imaginäre Teil gerade wird. Und man sieht leicht, dass unter vier associierten ungeraden Zahlen nur eine unter jener Form enthalten ist.

II. Wenn die Zahl $a+bi$ so beschaffen ist, dass $a-1$ und b entweder gleichzeitig geradernal gerade oder gleichzeitig ungerademal gerade sind, so wird ihr Product mit einer complexen Zahl von derselben Form dieselbe Eigenschaft besitzen, und man sieht leicht, dass von je vier associierten ungeraden Zahlen nur eine unter jener Form enthalten ist.

Von diesen beiden ungefähr gleich zweckmässigen Prinzipien werden wir das letztere wählen; wir werden nämlich unter vier associierten ungeraden complexen Zahlen diejenige als primäre Zahl betrachten, welche nach dem Modul $2+2i$ der positiven Einheit congruent wird; hierdurch werden wir mehrere ausgezeichnete Sätze in grösserer Kürze aussprechen können. So sind z. B. die complexen Primzahlen $-1+2i$, $-1-2i$, $+3+2i$, $+3-2i$, $+1+4i$, $+1-4i$, ... primäre Zahlen, ebenso die reellen -3, -7, -11, -19, ..., die offenbar immer mit negativem Vorzeichen zu versehen sind. Die zu einer ungeraden complexen primären Zahl conjugierte Zahl wird ebenfalls primäre Zahl sein.

Für halbgerade und gerade Zahlen im Allgemeinen würde eine ähnliche Unterscheidung allzu willkürlich und zu wenig nützlich sein. Von den associierten Primzahlen $1+i$, $1-i$, $-1+i$, $-1-i$ können wir zwar eine vor den übrigen als primäre Zahl auswählen, auf zusammengesetzte Zahlen werden wir aber eine solche Unterscheidung nicht ausdehnen.

37.

Wenn unter den Factoren einer zusammengesetzten complexen Zahl solche vorkommen, welche selbst zusammengesetzt sind, und diese wieder in ihre Factoren zerlegt werden, so wird man offenbar schliesslich zu Primfactoren kommen, d. h. jede zusammengesetzte Zahl ist in Primfactoren zerlegbar. Finden sich unter diesen welche, die nicht primäre Zahlen sind, so substituiere man an deren Stelle das Product aus der associierten primären Zahl in i, -1 oder $-i$. Auf diese Weise ergiebt sich, dass jede zusammengesetzte complexe Zahl M auf die Form reduciert werden kann:

$$M = i^{\mu} A^{\alpha} B^{\beta} C^{\gamma} \ldots,$$

derart, dass $A, B, C\ldots$ von einander verschiedene prime complexe primäre Zahlen sind und $\mu = 0, 1, 2$ oder 3 ist. Von einer solchen Zerlegung gilt der Satz, dass dieselbe nur auf eine einzige Weise möglich ist, ein Satz, der bei oberflächlicher Betrachtung allerdings an sich klar erscheinen könnte, aber jedenfalls eines Beweises bedarf. Zu diesem bahnt der folgende Satz den Weg.

Satz. Das Product $M = A^{\alpha} B^{\beta} C^{\gamma} \ldots$, in welchem $A, B, C, \ldots$ verschiedene prime complexe primäre Zahlen bezeichnen, kann

durch keine primäre complexe Primzahl teilbar sein, die nicht unter $A, B, C, \ldots$ enthalten ist.

Beweis. Es sei P eine primäre complexe Primzahl, die nicht unter $A, B, C, \ldots$ enthalten ist, und es seien $p, a, b, c \ldots$ die Normen der Zahlen $P, A, B, C \ldots$ Hieraus folgt leicht, dass die Norm der Zahl M gleich $a^\alpha b^\beta c^\gamma \ldots$ ist, so dass diese Zahl durch p teilbar sein müsste, wenn M durch p teilbar wäre. Da die einzelnen Normen entweder reelle Primzahlen (aus der Reihe 2, 5, 13, 17, ...) oder die Quadrate reeller Primzahlen (aus der Reihe 9, 49, 121, ...) sind, so ist unmittelbar klar, dass jenes nur stattfinden kann, wenn p mit irgend einer Norm $a, b, c \ldots$ identisch wird; wir nehmen daher $p = a$ an. Da aber nach Voraussetzung P und A von einander verschiedene primäre complexe Primzahlen sind, so sieht man leicht, dass dieses gleichzeitig nur bestehen kann, wenn P und A conjugierte complexe Zahlen sind und somit $p = a$ eine ungerade reelle Primzahl (nicht das Quadrat einer Primzahl) ist; wir setzen daher $A = k + li$, $P = k - li$. Hiernach wird (indem wir den Begriff und die Bezeichnung der Congruenz auf ganze complexe Zahlen ausdehnen) $A \equiv 2k$ (mod. P), woraus leicht folgt:

$$M \equiv 2^\alpha k^\alpha B^\beta C^\gamma \ldots \text{ (mod. } P).$$

Sobald also M durch P teilbar angenommen wird, wird auch

$$2^\alpha k^\alpha B^\beta C^\gamma \ldots$$

durch P teilbar und somit auch die Norm dieser Zahl, welche gleich

$$2^{2\alpha} k^{2\alpha} b^\beta c^\gamma \ldots$$

ist, durch p teilbar sein. Da aber 2 und k durch p sicher nicht teilbar sind, so folgt hieraus, dass p mit irgend einer der Zahlen $b, c \ldots$ identisch sein muss. Es sei z. B. $p = b$. Hieraus schliessen wir aber, dass entweder $B = k + li$ oder $B = k - li$, d. h. entweder $B = A$ oder $B = P$ ist, was beides der Voraussetzung widerspricht.

Aus diesem Satze leitet man den andern, dass die Zerlegung in Primfactoren nur auf eine einzige Weise möglich ist, sehr leicht her, und zwar durch Schlüsse, die denen, welche wir in den „*Arithmetischen Untersuchungen*" (Artikel 16, vgl. oben S. 7) benutzt haben, vollkommen analog sind; daher würde es überflüssig sein, uns hier damit aufzuhalten.

38.

Wir gehen jetzt zu der Congruenz der Zahlen nach complexen Moduln über. Am Eingange dieser Untersuchung ist es aber zweckmässig anzugeben, auf welche Weise die complexen Zahlen veranschaulicht werden können.

Ebenso wie jede reelle Grösse durch einen von einem willkürlichen Anfangspunkte aus zu nehmenden und nach einem willkürlichen als Einheit genommenen Segmente abzumessenden Teile einer nach beiden Seiten unendlichen geraden Linie ausgedrückt und somit durch den andern End-

punkt desselben dargestellt werden kann derart, dass die Punkte auf der einen Seite des Anfangspunktes die positiven, die Punkte auf der andern Seite die negativen Grössen repräsentieren, so kann auch jede complexe Grösse dargestellt werden durch irgend einen Punkt in einer unendlichen Ebene, in welcher eine bestimmte Gerade zur Darstellung der reellen Grössen dient, nämlich die complexe Grösse $x+iy$ durch einen Punkt, dessen Abscisse gleich x und dessen Ordinate (auf der einen Seite der Abscissenlinie positiv, auf der andern negativ genommen) gleich y ist. Auf diese Weise kann gesagt werden, dass jede beliebige complexe Grösse den Unterschied zwischen der Lage des Punktes, zu dem sie gehört, und der Lage des Anfangspunktes messe, wenn die positive Einheit eine willkürliche aber bestimmte Abweichung nach einer willkürlichen aber bestimmten Richtung hin, die negative Einheit eine ebenso grosse Abweichung nach der entgegengesetzten Richtung, endlich die imaginären Einheiten ebenso grosse Abweichungen nach zwei darauf senkrechten nach beiden Seiten gehenden Richtungen hin bezeichnen.

Auf diese Weise wird die Methaphysik der Grössen, welche wir imaginäre nennen, in ein ausgezeichnetes Licht gestellt. Wenn der Anfangspunkt mit (0) bezeichnet wird, und die beiden complexen Grössen m, m' sich auf die Punkte M, M' beziehen, deren Lagen in Bezug auf den Punkt (0) sie ausdrücken, so wird die Differenz $m-m'$ nichts anderes ausdrücken als die Lage des Punktes M in Bezug auf den Punkt M'; andrerseits wird man, wenn das Product mm' die Lage des Punktes N in Bezug auf (0) darstellt, leicht einsehen, dass diese Lage ebenso bestimmt wird durch die Lage des Punktes M in Bezug auf (0), wie die Lage des Punktes M' durch die Lage desjenigen Punktes, welchem die positive Einheit entspricht, bestimmt wird, so dass man nicht unpassend sagen kann, die Lagen der den complexen Grössen mm', m, m', 1 entsprechenden Punkte bilden eine Proportion. Doch behalten wir uns eine ausführlichere Behandlung dieses Gegenstandes für eine andere Gelegenheit vor. Die Schwierigkeiten, mit denen man die Theorie der imaginären Grössen umgeben geglaubt hat, haben ihren Grund grossenteils in den wenig schicklichen Benennungen (sind sie doch sogar von Einigen mit dem missklingenden Namen unmöglicher Grössen belegt worden). Hätte man, ausgehend von den Vorstellungen, welche Mannigfaltigkeiten von zwei Dimensionen (wie sie in grösster Reinheit in den räumlichen Anschauungen erblickt werden) darbieten, die positiven Grössen directe, die negativen inverse, die imaginären laterale Grössen genannt, so wäre Einfachheit anstatt Verwirrung, Klarheit anstatt Dunkelheit die Folge gewesen.

39.

Das im vorigen Artikel Vorgetragene bezieht sich auf stetige complexe Grössen; in der Arithmetik, welche es nur mit ganzen Zahlen zu thun hat, ist das Schema der complexen Zahlen ein System äquidistanter Punkte,

welche auf äquidistanten Geraden so gelegen sind, dass sie die unendliche Ebene in unendlich viele Quadrate zerlegen. Alle durch eine gegebene complexe Zahl $a + bi = m$ teilbaren Zahlen werden ebenfalls unendlich viele Quadrate bilden, deren Seite gleich $\sqrt{a^2 + b^2}$ oder deren Flächeninhalt gleich $a^2 + b^2$ ist; die letzteren Quadrate werden gegen die ersteren eine geneigte Lage haben, wenn keine der beiden Zahlen a, b gleich Null ist. Einer jeden durch den Modul m nicht teilbaren Zahl wird ein Punkt entsprechen, der entweder innerhalb eines solchen Quadrates oder auf der Grenzlinie zweier Quadrate liegt; der letztere Fall aber kann nur stattfinden, wenn a, b einen gemeinschaftlichen Teiler haben; ferner ist klar, dass die nach dem Modul m congruenten Zahlen in ihren Quadraten congruente Lagen einnehmen. Hieraus folgt leicht, dass, wenn man alle innerhalb eines bestimmten Quadrats gelegenen Zahlen sowie alle diejenigen, welche etwa auf zwei nicht gegenüberliegenden Seiten desselben liegen, sammelt und zu diesen endlich die durch m teilbare Zahl hinzurechnet, man ein vollständiges System nach dem Modul m incongruenter Reste erhält, d. h. dass jede ganze Zahl irgend einem von jenen und nur einem einzigen congruent sein muss. Es würde auch nicht schwierig sein zu zeigen, dass die Anzahl dieser Reste der Norm des Moduls gleich, nämlich gleich $a^2 + b^2$ ist. Doch scheint es ratsam, diesen sehr wichtigen Satz auf eine andere rein arithmetische Art zu beweisen.

40.

Satz. Nach dem gegebenen complexen Modul $m = a + bi$, dessen Norm $a^2 + b^2 = p$ ist und für welchen a, b zu einander prime Zahlen sind, wird jede beliebige ganze complexe Zahl irgend einem Reste aus der Reihe $0, 1, 2, 3, \ldots, p-1$ und nicht mehreren congruent sein.

Beweis. I. Sind α, β ganze Zahlen, für welche $\alpha a + \beta b = 1$ wird, so ist:

$$i = \alpha b - \beta a + m(\beta + \alpha i).$$

Ist daher eine ganze complexe Zahl $A + Bi$ gegeben, so hat man:

$$A + Bi = A + (\alpha b - \beta a)B + m(\beta B + \alpha Bi).$$

Bezeichnet man daher mit h den kleinsten positiven Rest der Zahl $A + (\alpha b - \beta a)B$ nach dem Modul p und setzt man:

$$A + (\alpha b - \beta a)B = h + kp = h + m(ak - bki),$$

so wird:

$$A + Bi = h + m[\beta B + ak + (\alpha B - bk)i]$$

oder:

$$A + Bi \equiv h \pmod{m}.$$

Damit ist der erste Teil des Satzes bewiesen.

II. Wenn derselben complexen Zahl zwei reelle Zahlen h, h' nach dem Modul m congruent sind, so werden sie auch unter einander congruent sein. Setzen wir daher $h - h' = m(c + di)$, so wird:

$$(h - h')(a - bi) = p(c + di)$$

und daher:

$$(h - h')a = pc, \ (h - h')b = -pd,$$

und ferner wegen $a\alpha + b\beta = 1$:

$$h - h' = p(c\alpha - d\beta), \text{ d. h. } h \equiv h' \ (\text{mod. } p).$$

Mithin können h und h', wofern sie ungleich sind, nicht beide gleichzeitig in dem Complex der Zahlen $0, 1, 2, 3, \ldots, p-1$ enthalten sein. Damit ist der zweite Teil des Satzes bewiesen.

41.

Satz. Nach dem complexen Modul $m = a + bi$, dessen Norm $a^2 + b^2 = p$ ist und für welchen a, b nicht prim zu einander sind, sondern den grössten gemeinschaftlichen Teiler λ (den wir positiv voraussetzen) haben, ist jede beliebige complexe Zahl einem Reste $x + iy$ von solcher Beschaffenheit congruent, dass x irgend eine der Zahlen $0, 1, 2, 3, \ldots, \frac{p}{\lambda} - 1$ und y irgend eine der Zahlen $0, 1, 2, 3, \ldots, \lambda - 1$ ist, und zwar nur einem einzigen unter allen p Resten, welche eine solche Form besitzen.

Beweis. I. Nimmt man die ganzen Zahlen α, β so an, dass $\alpha a + \beta b = \lambda$ wird, so ist:

$$\lambda i = \alpha b - \beta a + m(\beta + \alpha i).$$

Ist nun $A + Bi$ die gegebene complexe Zahl, ist ferner y der kleinste positive Rest von B nach dem Modul λ und x der kleinste positive Rest von $A + (\alpha b - \beta a)\frac{B - y}{\lambda}$ nach dem Modul $\frac{p}{\lambda}$, und setzt man:

$$A + (\alpha b - \beta a)\frac{B - y}{\lambda} = x + \frac{p}{\lambda} \cdot k,$$

so wird

$$\begin{aligned} A + Bi - (x + yi) &= \frac{p}{\lambda} \cdot k + (B - y)i - (\alpha b - \beta a)\frac{B - y}{\lambda} \\ &= \frac{p}{\lambda} \cdot k + \frac{B - y}{\lambda} \cdot m(\beta + \alpha i) \\ &= \left(\frac{a}{\lambda} - \frac{b}{\lambda} i\right) km + \frac{B - y}{\lambda}(\beta + \alpha i)m, \end{aligned}$$

d. h. durch m teilbar, oder $A + Bi \equiv x + yi$ (mod. m). Damit ist der erste Teil des Satzes bewiesen.

II. Nehmen wir an, dass nach dem Modul m derselben complexen Zahl zwei Zahlen $x+yi$ und $x'+y'i$ congruent seien, so werden dieselben auch unter einander nach dem Modul m congruent sein. Um so mehr also werden sie nach dem Modul λ congruent und daher $y \equiv y'$ (mod. λ) sein. Wenn man nun annimmt, dass jede der beiden Zahlen y, y' unter den Zahlen $0, 1, 2, 3, \ldots, \lambda-1$ enthalten sei, so muss notwendig $y=y'$ sein. Auf diese Weise aber wird auch $x \equiv x'$ (mod. m), d. h. $x-x'$ durch m teilbar und daher $\frac{x-x'}{\lambda}$ eine ganze durch $\frac{a}{\lambda}+\frac{b}{\lambda}i$ teilbare Zahl sein, oder es ist:

$$\frac{x-x'}{\lambda} \equiv 0 \left(\text{mod.}\ \frac{a}{\lambda}+\frac{b}{\lambda}i\right).$$

Hieraus aber folgt, da $\frac{a}{\lambda}$, $\frac{b}{\lambda}$ zu einander prime Zahlen sind, nach dem zweiten Teile des vorhergehenden Satzes, dass $\frac{x-x'}{\lambda}$ auch durch die Norm der Zahl $\frac{a}{\lambda}+\frac{b}{\lambda}i$, d. h. durch die Zahl $\frac{p}{\lambda^2}$ und somit auch $x-x'$ durch $\frac{p}{\lambda}$ teilbar ist. Daher wird, wenn man annimmt, dass auch jede der beiden Zahlen x, x' in dem Complex der Zahlen $0, 1, 2, 3, \ldots, \frac{p}{\lambda}-1$ enthalten sei, notwendig $x=x'$ oder die Reste $x+yi$, $x'+y'i$ werden identisch sein. Damit ist der zweite Teil des Satzes bewiesen.

Übrigens ist unmittelbar klar, dass hierher auch der Fall zu rechnen ist, wo der Modul eine reelle Zahl, also $b=0$ und somit $\lambda=\pm a$ ist, sowie der, wo der Modul eine rein imaginäre Zahl, also $a=0$ und somit $\lambda=\pm b$ ist. In beiden Fällen hat man $\frac{p}{\lambda}=\lambda$.

42.

Rechnet man daher alle nach einem gegebenen Modul unter einander congruenten complexen Zahlen zu derselben Klasse, incongruente aber zu verschiedenen Klassen, so wird es überhaupt p Klassen geben, welche die Gesamtheit der ganzen Zahlen erschöpfen, wenn p die Norm des Moduls bezeichnet. Der Complex von ebenso vielen aus den einzelnen Klassen entnommenen Zahlen wird ein vollständiges System incongruenter Reste darstellen, wie wir es in den Artikeln 40 und 41 bestimmt haben. Und zwar war in jenem Systeme die Wahl der die betreffenden Klassen gewissermassen repräsentierenden Reste auf das Prinzip gegründet worden, dass in jeder Klasse ein solcher Rest $x+yi$ genommen werden sollte, für welchen y den kleinsten Wert hat und unter allen, in welchen derselbe kleinste Wert von y vorkommt, derjenige, für welchen der Wert von x am kleinsten ist, mit Ausschluss aber von negativen Werten sowohl für x als

auch für y. Für andere Zwecke aber wird es zweckmässig sein, sich anderer Prinzipien zu bedienen, und zwar ist insbesondere die Art zu merken, wo solche Reste genommen werden, welche durch den Modul dividiert, die einfachsten Quotienten darbieten. Offenbar werden, wenn $\alpha+\beta i$, $\alpha'+\beta' i$, $\alpha''+\beta'' i\ldots$ die Quotienten sind, welche aus der Division congruenter Zahlen durch den Modul entstehen, sowohl die Differenzen der Grössen $\alpha, \alpha', \alpha'', \ldots$ unter einander als auch die Differenzen zwischen den Grössen $\beta, \beta', \beta'', \ldots$ ganze Zahlen sein, und es ist klar, dass stets ein Rest existiert, für welchen α und β zwischen den Grenzen 0 und 1, die erstere Grenze eingeschlossen, die letztere Grenze ausgeschlossen, liegen; einen solchen Rest werden wir einfach den **kleinsten Rest** nennen. Wenn man lieber will, kann man an Stelle jener Grenzen auch die folgenden $-\frac{1}{2}$ und $+\frac{1}{2}$ (die erstere eingeschlossen, die letztere ausgeschlossen) nehmen; einen dieser Beschränkung entsprechenden Rest werden wir den **absolut kleinsten Rest** nennen.

In Bezug auf diese kleinsten Reste bieten sich folgende Aufgaben dar.

43.

Den kleinsten Rest einer gegebenen complexen Zahl $A+Bi$ nach dem Modul $a+bi$, dessen Norm gleich p ist, findet man folgendermassen.

Ist $x+yi$ der gesuchte kleinste Rest, so wird $(x+yi)(a-bi)$ der kleinste Rest des Products $(A+Bi)(a-bi)$ nach dem Modul $(a+bi)(a-bi)$, d. h. nach dem Modul p sein. Setzt man daher:

$$aA+bB=Fp+f,\quad aB-bA=Gp+g,$$

so dass f, g die kleinsten Reste der Zahlen $aA+bB$, $aB-bA$ nach dem Modul p sind, so ist:

$$x+yi=\frac{f+gi}{a-bi}$$

oder:

$$x=\frac{af-bg}{p}=A-aF+bG$$

$$y=\frac{ag+bf}{p}=B-aG-bF.$$

Offenbar müssen die kleinsten Reste f, g entweder zwischen den Grenzen 0 und $p-1$ oder zwischen den Grenzen $-\frac{1}{2}p$ und $+\frac{1}{2}p$ genommen werden, je nachdem entweder einfach der kleinste Rest oder der absolut kleinste Rest der complexen Zahl verlangt wird.

44.

Die Aufstellung des vollständigen Systems der kleinsten Reste für einen gegebenen Modul kann auf mehrere Arten ausgeführt

werden. Das erste Verfahren geht in der Weise vor, dass zuerst die Grenzen bestimmt werden, innerhalb deren die reellen Glieder liegen müssen, und sodann für die einzelnen innerhalb dieser Grenzen liegenden Werte die Grenzen der imaginären Teile festgestellt werden. Das allgemeine Kriterium eines kleinsten Restes $x+yi$ für den Modul $a+bi$ besteht darin, dass sowohl $ax+by=\xi$ als auch $ay-bx=\eta$ zwischen den Grenzen 0 und a^2+b^2 liegt, wenn es sich einfach um die kleinsten Reste handelt, oder zwischen den Grenzen $-\frac{1}{2}(a^2+b^2)$ und $+\frac{1}{2}(a^2+b^2)$, wenn die absolut kleinsten Reste verlangt werden, wobei die zweite Grenze ausgeschlossen ist. Specielle Regeln würden die Unterscheidung der Fälle, welche die Verschiedenheit der Vorzeichen der Zahlen a, b veranlasst, erfordern, doch überheben wir uns hier der Mühe, uns mit der Entwicklung derselben, welche keinen Schwierigkeiten unterworfen ist, abzugeben. Es möge genügen, die Natur des Verfahrens an einem einzigen **Beispiele** dargelegt zu haben.

Für den Modul $5+2i$ müssen die einfach kleinsten Reste $x+yi$ so beschaffen sein, dass sowohl $5x+2y=\xi$ als auch $5y-2x=\eta$ gleich irgend einer der Zahlen $0, 1, 2, 3, \ldots, 28$ ist. Die Gleichung $29x=5\xi-2\eta$ zeigt, dass die positiven Werte von x nicht grösser als $\frac{5\cdot 28}{29}$, die negativen, vom Vorzeichen abgesehen, nicht grösser als $\frac{2\cdot 28}{29}$ sein können. Daher sind die sämtlichen zulässigen Werte von x die folgenden: $-1, 0, 1, 2, 3, 4$. Für $x=-1$ muss $2y$ gleich irgend einem der Werte $5, 6, 7, \ldots, 33$ und $5y$ irgend einem der Werte $-2, -1, 0, 1, \ldots, 26$ gleich sein; daher ist der kleinste Wert von y gleich $+3$, der grösste gleich $+5$. Behandelt man ebenso die übrigen Werte von x, so ergiebt sich folgendes Schema aller kleinsten Reste:

x	y
-1	3, 4, 5
0	0, 1, 2, 3, 4, 5
$+1$	1, 2, 3, 4, 5, 6
$+2$	1, 2, 3, 4, 5, 6
$+3$	2, 3, 4, 5, 6
$+4$	2, 3, 4.

In ähnlicher Weise müssen für die absolut kleinsten Reste ξ und η irgend einer der Zahlen $-14, -13, -12, \ldots, +14$ gleich sein; hiernach kann nicht $29x$ ausserhalb der Grenzen $-7\cdot 14$ und $+7\cdot 14$ liegen, und daher muss x irgend einer der Zahlen $-3, -2, -1, 0, 1, 2, 3$ gleich sein. Für $x=-3$ wird $2y=\xi-5x=\xi+15$ irgend einer der Zahlen $1, 2, 3, \ldots, 29$ gleich, $5y=\eta+2x=\eta-6$ aber irgend einer der Zahlen $-20, -19, -18, \ldots, +8$. Hieraus ergiebt sich für y der

einzige Wert $+1$. Behandelt man die übrigen Werte von x in derselben Weise, so erhält man das Schema sämtlicher absolut kleinsten Reste:

x	y
-3	$+1$
-2	$-2, -1, 0, +1, +2$
-1	$-3, -2, -1, 0, +1, +2$
0	$-2, -1, 0, +1, +2$
$+1$	$-2, -1, 0, +1, +2, +3$
$+2$	$-2, -1, 0, +1, +2$
$+3$	$-1.$

45.

Bei der Anwendung der zweiten Methode ist es zweckmässig, zwei Fälle zu unterscheiden.

In dem ersten Falle, in welchem a und b keinen gemeinschaftlichen Teiler haben, werde $\alpha a + \beta b = 1$ gesetzt, und es sei k der kleinste positive Rest von $\beta a - \alpha b$ nach dem Modul p. Hiernach zeigen die identischen Relationen

$$a(\beta a - \alpha b) = \beta p - b(\alpha a + \beta b), \quad b(\beta a - \alpha b) = -\alpha p + a(\alpha a + \beta b),$$

dass $ak \equiv -b$, $bk \equiv a \pmod{p}$ ist. Setzt man daher wie oben $ax + by = \xi$, $ay - bx = \eta$, so ist $\eta \equiv k\xi$, $\xi \equiv -k\eta \pmod{p}$. Man erhält somit alle Zahlen $\xi + \eta i$, welche den einfach kleinsten Resten $x + yi$ entsprechen, wenn man entweder für ξ der Reihe nach die Werte $0, 1, 2, 3, \ldots, p-1$ und für η die kleinsten positiven Reste der Producte $k\xi$ nach dem Modul p oder umgekehrt für η jene Werte und für ξ die kleinsten Reste der Producte $-k\eta$ nimmt. Aus den einzelnen $\xi + \eta i$ findet man dann die entsprechenden $x + yi$ nach der Formel:

$$x + yi = \frac{\xi + \eta i}{a - bi} = \frac{a\xi - b\eta}{p} + \frac{a\eta + b\xi}{p} i.$$

Ferner ist klar, dass η, während ξ um die Einheit wächst, entweder den Zuwachs k oder die Verminderung $p - k$ und daher $x + yi$

entweder die Änderung $\dfrac{a - kb}{p} + \dfrac{ak + b}{p} i$

oder die folgende $\dfrac{a - kb}{p} + b + \left(\dfrac{ak + b}{p} - a\right) i$

erleidet, eine Bemerkung, welche dazu dient, die Aufstellung zu erleichtern.

Endlich werden, wenn die absolut kleinsten Reste $x + yi$ verlangt werden, diese Vorschriften nur insofern sich ändern, als jetzt ξ der Reihe nach die Werte zwischen den Grenzen $-\frac{1}{2}p$ und $+\frac{1}{2}p$ beizulegen sind, während für η die absolut kleinsten Reste der Producte $k\xi$ genommen werden

müssen. Es folgt hier das Schema der auf diese Weise erhaltenen kleinsten Reste für den Modul $5+2i$.

Einfach kleinste Reste.

$\xi+\eta i$	$x+yi$	$\xi+\eta i$	$x+yi$	$\xi+\eta i$	$x+yi$
0	0	$10+25i$	$+5i$	$20+21i$	$+2+5i$
$1+17i$	$-1+3i$	$11+13i$	$+1+3i$	$21+9i$	$+3+3i$
$2+5i$	$+i$	$12+i$	$+2+i$	$22+26i$	$+2+6i$
$3+22i$	$+1+4i$	$13+18i$	$+1+4i$	$23+14i$	$+3+4i$
$4+10i$	$+2i$	$14+6i$	$+2+2i$	$24+2i$	$+4+2i$
$5+27i$	$-1+5i$	$15+23i$	$+1+5i$	$25+19i$	$+3+5i$
$6+15i$	$+3i$	$16+11i$	$+2+3i$	$26+7i$	$+4+3i$
$7+3i$	$+1+i$	$17+28i$	$+1+6i$	$27+24i$	$+3+6i$
$8+20i$	$+4i$	$18+16i$	$+2+4i$	$28+12i$	$+4+4i.$
$9+8i$	$+1+2i$	$19+4i$	$+3+2i$		

Absolut kleinste Reste.

$\xi+\eta i$	$x+yi$	$\xi+\eta i$	$x+yi$	$\xi+\eta i$	$x+yi$
$-14-6i$	$-2-2i$	$-4-10i$	$-2i$	$+5-2i$	$+1$
$-13+11i$	$-3+i$	$-3+7i$	$-1+i$	$+6-14i$	$+2-2i$
$-12-i$	$-2-i$	$-2-5i$	$-i$	$+7+3i$	$+1+i$
$-11-13i$	$-1-3i$	$-1+12i$	$-1+2i$	$+8-9i$	$+2-i$
$-10+4i$	-2	0	0	$+9+8i$	$+1+2i$
$-9-8i$	$-1-2i$	$+1-12i$	$+1-2i$	$+10-4i$	$+2$
$-8+9i$	$-2+i$	$+2+5i$	$+i$	$+11+13i$	$+1+3i$
$-7-3i$	$-1-i$	$+3-7i$	$+1-i$	$+12+i$	$+2+i$
$-6+14i$	$-2+2i$	$+4+10i$	$+2i$	$+13-11i$	$+3-i$
$-5+2i$	-1			$+14+6i$	$+2+2i.$

Den zweiten Fall, in welchem a, b nicht prim zu einander sind, kann man leicht auf den vorhergehenden Fall zurückführen. Es sei λ der grösste gemeinschaftliche Teiler der Zahlen a, b, und $a = \lambda a'$, $b = \lambda b'$. Es bezeichne ferner F unbestimmt den kleinsten Rest für den Modul λ, insofern derselbe als complexe Zahl betrachtet wird, d. h. es stelle F unbestimmt eine solche Zahl $x+yi$ dar, dass x, y entweder zwischen den Grenzen 0 und λ oder zwischen den Grenzen $-\frac{1}{2}\lambda$ und $+\frac{1}{2}\lambda$ liegen (je nachdem es sich um die einfach kleinsten oder absolut kleinsten Reste handelt); endlich bezeichne F' unbestimmt den kleinsten Rest für den Modul $a'+b'i$. Dann ist $(a'+b'i)F+F'$ unbestimmt der kleinste Rest für den Modul $a+bi$, und das vollständige System dieser Reste wird man erhalten, wenn man sämtliche F mit sämtlichen F' combiniert.

46.

Zwei complexe Zahlen werden zu einander **prim** genannt, wenn sie ausser den Einheiten keine andern gemeinschaftlichen Teiler besitzen; sooft aber derartige gemeinschaftliche Teiler vorhanden sind, so werden diejenigen die grössten gemeinschaftlichen Teiler genannt, deren Norm am grössten ist.

Wenn die Zerlegung zweier gegebenen Zahlen in Primfactoren gegeben ist, so wird die Bestimmung des grössten gemeinschaftlichen Teilers auf genau dieselbe Weise ausgeführt, wie bei den reellen Zahlen (*Arithmetische Untersuchungen,* Artikel 18, vgl. oben S. 8). Zugleich geht hieraus hervor, dass sämtliche gemeinschaftlichen Teiler zweier gegebenen Zahlen auch in dem grössten auf diese Weise gefundenen gemeinschaftlichen Teiler derselben aufgehen müssen. Da nun bereits von selbst klar ist, dass die drei diesem associierten Zahlen ebenfalls gemeinschaftliche Teiler sein werden, so werden stets je vier und nicht mehr grösste gemeinschaftliche Teiler genannt werden müssen, und die Norm dieser wird ein Vielfaches jedes andern gemeinschaftlichen Teilers sein.

Wenn die Zerlegung zweier gegebenen Zahlen in einfache Factoren nicht gegeben ist, so findet man den grössten gemeinschaftlichen Teiler mit Hülfe eines ähnlichen Algorithmus, wie für reelle Zahlen. Es seien m, m' die beiden gegebenen Zahlen und man bilde durch wiederholte Division die Reihe $m'', m''', \ldots$ derart, dass m'' der absolut kleinste Rest von m nach dem Modul m', ferner m''' der absolut kleinste Rest von m' nach dem Modul m'' ist, u. s. f. Bezeichnet man die Normen der Zahlen $m, m', m'', m''', \ldots$ respective mit $p, p', p'', p''', \ldots$, so ist $\frac{p''}{p'}$ die Norm des Quotienten $\frac{m''}{m'}$ und daher nach der Definition des absolut kleinsten Restes sicher nicht grösser als $\frac{1}{2}$; dasselbe gilt von $\frac{p'''}{p''}$, u. s. w. Mithin werden die positiven reellen ganzen Zahlen $p', p'', p''', \ldots$ eine beständig abnehmende Reihe bilden, so dass man notwendig schliesslich zu dem Gliede 0 oder, was dasselbe ist, in der Reihe $m, m', m'', m''', \ldots$ schliesslich zu einem Gliede gelangt, welches in dem vorhergehenden ohne Rest aufgeht. Es sei dieses Glied $m^{(n+1)}$ und es werde gesetzt:

$$\begin{aligned} m &= km' + m'' \\ m' &= k'm'' + m''' \\ m'' &= k''m''' + m'''' \\ &\ldots\ldots\ldots \quad \text{bis zu} \\ m^{(n)} &= k^{(n)}m^{(n+1)}. \end{aligned}$$

Durchläuft man diese Reihe von Gleichungen in umgekehrter Ordnung, so ergiebt sich, dass $m^{(n+1)}$ in jedem einzelnen der vorhergehenden Glieder

$m^{(n)}, \ldots, m'', m', m$ aufgeht. Durchläuft man aber dieselben Gleichungen in directer Reihenfolge, so ist ersichtlich, dass jeder gemeinschaftliche Teiler der Zahlen m, m' auch in jedem der folgenden aufgeht. Der erste Schluss lehrt, dass $m^{(n+1)}$ ein gemeinschaftlicher Teiler der Zahlen m, m' ist, der letzte aber, dass dieser Teiler der grösste ist.

Sooft übrigens der letzte Rest $m^{(n+1)}$ irgend einer der vier Einheiten 1, $-1, i, -i$ gleich wird, so ist dies ein Zeichen dafür, dass m und m' unter einander prim sind.

47.

Wenn man die Gleichungen des vorigen Artikels mit Weglassung der letzen derart mit einander combiniert, dass $m'', m''', m'''', \ldots, m^{(n)}$ eliminiert werden, so entsteht eine Gleichung von der Form:

$$m^{(n+1)} = hm + h'm',$$

wo h und h' ganze Zahlen sind und zwar, wenn man sich der in den *„Arithmetischen Untersuchungen"*, Artikel 27 (vgl. oben S. 12), eingeführten Bezeichnung bedienen will:

$$h = \pm [k', k'', k''', \ldots, \quad k^{(n-1)}] = \pm [k^{(n-1)}, \; k^{(n-2)}, \ldots k'', \; k']$$
$$h' = \mp [k, k', k'', k''', \ldots, k^{(n-1)}] = \mp [k^{(n-1)}, \; k^{(n-2)}, \ldots k'', \; k', \; k],$$

wobei die oberen oder unteren Vorzeichen gelten, je nachdem n gerade oder ungerade ist. Diesen **Satz** sprechen wir folgendermassen aus:

Der grösste gemeinschaftliche Teiler zweier complexen Zahlen m, m' lässt sich auf die Form $hm + h'm'$ bringen, so dass h und h' ganze Zahlen sind.

Offenbar nämlich gilt dieses nicht nur von demjenigen grössten gemeinschaftlichen Teiler, zu welchem der Algorithmus des vorigen Artikels geführt hat, sondern auch von den drei zu jenem associierten, für welche man an Stelle der Coefficienten h, h' entweder $hi, h'i$, oder $-h, -h'$, oder $-hi, -h'i$ nehmen muss.

Sobald daher die Zahlen m, m' zu einander prim sind, kann der Gleichung

$$1 = hm + h'm'$$

Genüge geleistet werden.

Es seien z. B. die Zahlen $31 + 6i = m$, $11 - 20i = m'$ gegeben. Hier finden wir:

$$\begin{aligned} k &= i, & m'' &= +11 - 5i \\ k' &= +1 - i, & m''' &= +5 - 4i \\ k'' &= +2, & m'''' &= +1 + 3i \\ k''' &= -1 - 2i, & m''''' &= +i \\ k'''' &= +3 - i, & & \end{aligned}$$

und hieraus:

$$[k', k'', k'''] \quad = -6 - \quad 5i$$
$$[k, k', k'', k'''] = +4 - 10i,$$

und somit:

$$m''''' = i = (6 + 5i)m + (4 - 10i)m',$$

sowie ferner:

$$1 = (5 - 6i)m + (-10 - 4i)m',$$

welche Gleichungen man durch wirkliche Ausrechnung leicht bestätigt.

48.

Durch das Vorhergehende ist alles, was zur Theorie der Congruenzen ersten Grades in der Arithmetik der complexen Zahlen erforderlich ist, vorbereitet worden; da aber jenes nicht wesentlich von demjenigen verschieden ist, was für die Arithmetik der reellen Zahlen gilt, und dieses in den „*Arithmetischen Untersuchungen*“ ausführlich dargelegt worden ist, so wird es genügen, wenn wir hier nur die Hauptmomente hinzufügen.

I. Die Congruenz $mt \equiv 1 \pmod{m'}$ ist der unbestimmten Gleichung $mt + m'u = 1$ äquivalent, und wenn dieser durch die Werte $t = h$, $u = h'$ genügt wird, so wird die Lösung jener allgemein dargestellt durch $t \equiv h \pmod{m'}$. Die Bedingung der Lösbarkeit aber ist die, dass der Modul m' mit dem Coefficienten m keinen gemeinschaftlichen Teiler habe.

II. Die Lösung der Congruenz $ax + b \equiv c \pmod{M}$ in dem Falle, wo a und M zu einander prim sind, hängt von der Lösung der folgenden ab:

$$at \equiv 1 \pmod{M};$$

wird dieser genügt durch $t = h$, so ist die allgemeine Lösung jener in der Formel enthalten:

$$x \equiv (c - b)h \pmod{M}.$$

III. Die Congruenz $ax + b \equiv c \pmod{M}$ in dem Falle, wo a und M einen gemeinschaftlichen Teiler λ haben, ist der folgenden äquivalent:

$$\frac{a}{\lambda}x \equiv \frac{c-b}{\lambda} \left(\mathrm{mod.}\, \frac{M}{\lambda}\right).$$

Sobald daher für λ der grösste gemeinschaftliche Teiler der Zahlen a und M genommen wird, reduciert sich die Lösung der gegebenen Gleichung auf den vorhergehenden Fall, und es ist klar, dass die zur Lösbarkeit der Congruenz erforderliche und hinreichende Bedingung die ist, dass λ auch in der Differenz $c - b$ aufgeht.

49.

Bisher haben wir nur elementare Dinge angeführt, die wir jedoch des Zusammenhanges wegen nicht weglassen durften. In den tieferen Untersuchungen ist die Arithmetik der complexen Zahlen der Arithmetik der

reellen Zahlen darin ähnlich, dass die Sätze einfacher und eleganter werden, wenn man nur solche Moduln, welche Primzahlen sind, zulässt; in Wirklichkeit ist die Ausdehnung derselben auf zusammengesetzte Moduln in den meisten Fällen mehr weitläufig als schwierig und erfordert mehr Arbeit als Kunst. Aus diesem Grunde soll im Folgenden insbesondere von Primzahlmoduln die Rede sein.

50.

Bezeichnet X eine Function der Unbestimmten x von der Form:

$$Ax^n + Bx^{n-1} + Cx^{n-2} + \cdots + Mx + N,$$

wo n eine reelle positive ganze Zahl, A, B, C, ... reelle oder imaginäre ganze Zahlen sind, und ist m eine ganze complexe Zahl, so werden wir auch hier **Wurzel der Congruenz** $X \equiv 0 \pmod{m}$ jede beliebige ganze Zahl nennen, welche, für x substituiert, einen durch den Modul m teilbaren Wert von X hervorbringt. Lösungen durch Wurzeln, welche nach dem Modul congruent sind, werden wir nicht als verschieden betrachten.

Ist der Modul eine Primzahl, so kann eine solche Congruenz von der Ordnung n auch hier nicht mehr als n verschiedene Lösungen besitzen. Bezeichnet α jede bestimmte (complexe) ganze Zahl, so kann X mittelst Division durch $x-\alpha$ unbestimmt auf die Form $X=(x-\alpha)X'+h$ gebracht werden, so dass h eine bestimmte ganze Zahl und X' eine Function von der $n-1^{\text{ten}}$ Ordnung mit ganzzahligen Coefficienten wird. Ist nun α eine Wurzel der Congruenz $X \equiv 0 \pmod{m}$, so wird offenbar h durch m teilbar sein, oder man wird für jeden Wert von x die Congruenz haben: $X \equiv (x-\alpha)X' \pmod{m}$.

Ebenso reduciert sich, wenn β eine bestimmte ganze Zahl bezeichnet, X' auf die Form: $(x-\beta)X''+h'$, wo X'' eine Function $n-2^{\text{ter}}$ Ordnung mit ganzzahligen Coefficienten ist. Nimmt man aber an, dass β eine Wurzel der Congruenz $X \equiv 0$ sei, so muss sie auch der Congruenz $(\beta-\alpha)X' \equiv 0$ genügen, sowie der folgenden $X' \equiv 0$, wofern die Wurzeln α, β incongruent sind, woraus wir schliessen, dass auch h' durch m teilbar oder unbestimmt $X \equiv (x-\alpha)(x-\beta)X'' \pmod{m}$ sein muss.

In analoger Weise erhalten wir, wenn eine dritte den ersteren incongruente Wurzel γ hinzutritt, $X \equiv (x-\alpha)(x-\beta)(x-\gamma)X'''$, so dass X''' eine Function $n-3^{\text{ter}}$ Ordnung mit ganzzahligen Coefficienten ist. Auf dieselbe Weise kann man weiter fortgehen, und zugleich ist klar, dass der Coefficient des höchsten Gliedes in den einzelnen Functionen gleich A ist, welches wir als durch m nicht teilbar voraussetzen dürfen, da sonst die Congruenz $X \equiv 0$ wesentlich zu einer niedrigeren Ordnung gerechnet werden müsste. Sind daher n incongruente Wurzeln vorhanden, nämlich $\alpha, \beta, \gamma, \ldots, \nu$, so haben wir unbestimmt:

$$X \equiv A(x-\alpha)(x-\beta)(x-\gamma)\ldots(x-\nu) \pmod{m};$$

mithin würde die Substitution eines neuen zu jeder der Grössen $\alpha, \beta, \gamma, \ldots, \nu$ incongruenten Wertes für X sicher einen durch m nicht teilbaren Wert liefern, woraus die Richtigkeit unseres Satzes von selbst folgt.

Übrigens stimmt dieser Beweis im Wesentlichen überein mit demjenigen, welchen wir in den „*Arithmetischen Untersuchungen*" Artikel 43 (vgl. oben S. 27) mitgeteilt haben, und dessen einzelnen Momente ebenso für complexe Zahlen gelten wir für reelle.

51.

Das, was in dem dritten Abschnitte der „*Arithmetischen Untersuchungen*" in Bezug auf die Reste der Potenzen mitgeteilt ist, gilt grösstenteils mit nur geringfügigen Änderungen auch in der Arithmetik dor complexen Zahlen; ja sogar die Beweise der Sätze könnten in den meisten Fällen beibehalten werden. Um es aber an nichts fehlen zu lassen, wollen wir die Hauptsätze, mit kurzen Beweisen versehen, anführen, wobei man sich stets zu denken hat, dass der Modul eine Primzahl ist.

Satz. Bezeichnet k eine ganze Zahl, welche durch den Modul m, dessen Norm gleich p sei, nicht teilbar ist, so ist $k^{p-1} \equiv 1 \pmod{m}$.

Beweis. Es mögen $a, b, c, \ldots$ ein vollständiges System incongruenter Reste für den Modul m bilden, so jedoch, dass der durch m teilbare Rest weggelassen ist, und daher die Anzahl jener Zahlen, deren Complex wir mit C bezeichnen, gleich $p-1$ ist. Es sei ferner C' der Complex der Producte $ka, kb, kc, \ldots$ Von diesen Producten ist nach Voraussetzung keins durch m teilbar, daher werden sie einzeln im Complexe C zu sich selbst congruente Reste haben, es wird also gesetzt werden können $ak \equiv a', bk \equiv b', ck \equiv c', \ldots \pmod{m}$ derart, dass die Zahlen $a', b', c', \ldots$ im Complexe C vorkommen. Wir bezeichnen den Complex der Zahlen $a', b', c', \ldots$ mit C''. Es seien ferner P, P', P'' die Producte aus den einzelnen Zahlen der Complexe C, C', C'', oder:

$$P = abc\ldots$$
$$P' = k^{p-1}abc\ldots = k^{p-1}P$$
$$P'' = a'b'c'\ldots$$

Da die Zahlen des Complexes C'' der Reihe nach den Zahlen des Complexes C' congruent sind, so ist $P'' \equiv P'$ oder $P'' \equiv k^{p-1}P$. Da man aber leicht sieht, dass irgend zwei Zahlen des Complexes C'' unter einander incongruent und daher alle unter einander verschieden sind, so stimmen notwendig die Zahlen des Complexes C'', nur in veränderter Reihenfolge, mit den Zahlen des Complexes C vollständig überein, und daher wird $P'' = P$. Es ist daher $(k^{p-1}-1)P$ eine durch m teilbare Zahl, wonach notwendig, da m eine Primzahl ist, welche in den einzelnen Factoren von P nicht aufgeht, $k^{p-1}-1$ durch m teilbar sein muss.

52.

Satz. Bezeichnet k wie im vorigen Artikel eine ganze durch den Modul m nicht teilbare Zahl und t den kleinsten Exponenten (ausser 0), für welchen $k^t \equiv 1 \pmod{m}$ ist, so ist t ein Teiler jedes andern Exponenten u, für welchen $k^u \equiv 1 \pmod{m}$ ist.

Beweis. Wäre t kein Teiler von u, so sei gt das Vielfache von t, welches nächstgrösser ist als u, und daher $gt - u$ eine ganze positive Zahl kleiner als t. Aus $k^t \equiv 1$, $k^u \equiv 1$ folgt: $0 \equiv k^{gt} - k^u \equiv k^u(k^{gt-u} - 1)$ und daher $k^{gt-u} \equiv 1$, d. h. es giebt eine Potenz von k mit einem kleineren Exponenten als t, welche der Einheit congruent ist. Dies widerspricht aber der Voraussetzung.

Als Corollar folgt hieraus, dass t sicher in $p-1$ aufgeht.

Derartige Zahlen k, für welche $t = p-1$ ist, werden wir auch hier **primitive** Wurzeln für den Modul m nennen. Dass es solche wirklich giebt, werden wir jetzt zeigen.

53.

Man zerlege die Zahl $p-1$ in ihre Primfactoren, so dass man hat:

$$p - 1 = a^\alpha b^\beta c^\gamma \ldots,$$

wo $a, b, c, \ldots$ von einander verschiedene positive reelle Primzahlen bezeichnen. Es seien ferner $A, B, C, \ldots$ ganze (complexe) durch m nicht teilbare Zahlen, welche respective den Congruenzen

$$x^{\frac{p-1}{a}} \equiv 1, \quad x^{\frac{p-1}{b}} \equiv 1, \quad x^{\frac{p-1}{c}} \equiv 1, \ldots.$$

nach dem Modul m **nicht** Genüge leisten; dass es solche giebt, ist aus dem Satze des Artikels 50 ersichtlich. Endlich sei h nach dem Modul m dem Producte

$$A^{\frac{p-1}{a^\alpha}} \cdot B^{\frac{p-1}{b^\beta}} \cdot C^{\frac{p-1}{c^\gamma}} \ldots.$$

congruent. Dann behaupte ich, dass h eine primitive Wurzel ist.

Beweis. Bezeichnet man mit t den Exponenten der niedrigsten der Einheit congruenten Potenz h^t, so ist, wenn h keine primitive Wurzel wäre, t ein Teiler von $p-1$ oder $\frac{p-1}{t}$ eine die Einheit übersteigende ganze Zahl. Offenbar befinden sich die reellen Primfactoren dieser ganzen Zahl unter den Zahlen $a, b, c, \ldots$ Wir nehmen daher (was erlaubt ist) an, dass $\frac{p-1}{t}$ durch a teilbar sei und setzen $p - 1 = atu$. Wegen $h^t \equiv 1$ ist daher auch $h^{tu} \equiv 1$ oder

$$A^{\frac{p-1}{a^\alpha} \cdot \frac{p-1}{a}} \cdot B^{\frac{p-1}{b^\beta} \cdot \frac{p-1}{a}} \cdot C^{\frac{p-1}{c^\gamma} \cdot \frac{p-1}{a}} \ldots \equiv 1.$$

Es ist aber offenbar $\frac{p-1}{ab^\beta}$ eine ganze Zahl und somit

$$B^{\frac{p-1}{b^\beta}\cdot\frac{p-1}{a}} = (B^{p-1})^{\frac{p-1}{ab^\beta}} \equiv 1;$$

ebenso auch:

$$C^{\frac{p-1}{c^\gamma}\cdot\frac{p-1}{c}} \equiv 1$$

u. s. w. Mithin muss sein:

$$A^{\frac{p-1}{a^\alpha}\cdot\frac{p-1}{a}} \equiv 1.$$

Man bestimme nun eine positive ganze Zahl λ derart, dass

$$\lambda b^\beta c^\gamma \ldots . \equiv 1 \text{ (mod. } a)$$

wird, was möglich ist, da die Primzahl a in der Zahl $b^\beta c^\gamma \ldots$ nicht aufgeht, und setze $\lambda b^\beta c^\gamma \ldots = 1 + a\mu$. Dann wird offenbar:

$$A^{\lambda\cdot\frac{p-1}{a^\alpha}\cdot\frac{p-1}{a}} \equiv 1, \text{ oder, da } \lambda\cdot\frac{p-1}{a^\alpha}\cdot\frac{p-1}{a} = (1+a\mu)\frac{p-1}{a}$$
$$= (p-1)\mu + \frac{p-1}{a} \text{ ist:}$$

$$A^{(p-1)\mu}\cdot A^{\frac{p-1}{a}} \equiv 1,$$

und hieraus folgt, da $A^{(p-1)\mu} \equiv 1$ ist, auch $A^{\frac{p-1}{a}} \equiv 1$, was im Widerspruch steht mit der Voraussetzung. Mithin kann die Annahme, dass t ein Teiler von $p-1$ sei, nicht bestehen und somit ist notwendig h eine primitive Wurzel.

54.

Bezeichnet h eine primitive Wurzel für den Modul m, dessen Norm gleich p sei, so werden die Glieder der Reihe

$$1, h, h^2, h^3, \ldots, h^{p-2}$$

einander incongruent sein, woraus leicht folgt, dass jede ganze durch den Modul nicht teilbare Zahl einer von jenen Zahlen congruent sein muss oder dass jene Reihe ein vollständiges System incongruenter Reste mit Ausschluss der Null darstellt. Der Exponent derjenigen Potenz, welcher eine gegebene Zahl congruent ist, kann der **Index** dieser Zahl genannt werden, wenn h als **Basis** betrachtet wird. Wir geben hier einige Beispiele an, wobei wir neben jeden Index den absolut kleinsten Rest gesetzt haben.

Erstes Beispiel.

$m = 5 + 4i, \quad p = 41, \quad h = 1 + 2i$

Index	Rest	Index	Rest	Index	Rest	Index	Rest	Index	Rest
0	$+1$	8	-4	16	$-2+2i$	24	$+2i$	32	$+1+i$
1	$+1+2i$	9	$-3+i$	17	$-1+2i$	25	$-3i$	33	$+1+3i$
2	$+1-i$	10	$-i$	18	$+4i$	26	$+2+2i$	34	$+2$
3	$+3+i$	11	$+2-i$	19	$+1+3i$	27	$+2+i$	35	-3
4	$-2i$	12	$-1-i$	20	-1	28	$+4$	36	$+2-2i$
5	$+3i$	13	$+1-3i$	21	$-1-2i$	29	$+3-i$	37	$+1-2i$
6	$-2-2i$	14	-2	22	$-1+i$	30	$+i$	38	$-4i$
7	$-2-i$	15	$+3$	23	$-3-i$	31	$-2+i$	39	$-1-3i$

Zweites Beispiel.

$m = 7, \quad p = 49, \quad h = 1 + 2i.$

Index	Rest	Index	Rest	Index	Rest	Index	Rest	Index	Rest
0	$+1$	10	$-1-i$	20	$+2i$	30	$+2-2i$	40	$+3$
1	$+1+2i$	11	$+1-3i$	21	$+3+2i$	31	$-1+2i$	41	$+3-i$
2	$-3-3i$	12	$-i$	22	$-1+i$	32	$+2$	42	$-2-2i$
3	$+3-2i$	13	$+2-i$	23	$-3-i$	33	$+2-3i$	43	$+2+i$
4	$-3i$	14	$-3+3i$	24	-1	34	$+1+i$	44	$-2i$
5	$-1-3i$	15	$-2-3i$	25	$-1-2i$	35	$-1+3i$	45	$-3-2i$
6	$-2+2i$	16	-3	26	$+3+3i$	36	$+i$	46	$+1-i$
7	$+1-2i$	17	$-3+i$	27	$-3+2i$	37	$-2+i$	47	$+3+i$
8	-2	18	$+2+2i$	28	$+3i$	38	$+3-3i$		
9	$-2+3i$	19	$-2-i$	29	$+1+3i$	39	$+2+3i$		

55.

Wir fügen in Bezug auf die primitiven Wurzeln und den Algorithmus der Indices einige Bemerkungen hinzu, lassen aber die Beweise ihrer Leichtigkeit wegen fort.

I. Nach dem Modul $p-1$ congruente Indices entsprechen in einem gegebenen System nach dem Modul m congruenten Resten und umgekehrt.

II. Reste, welche zu $p-1$ primen Indices entsprechen, sind ebenfalls primitive Wurzeln und umgekehrt.

III. Hat man eine primitive Wurzel h zur Basis genommen und ist t der Index einer andern primitiven Wurzel h' und umgekehrt t' der Index von h, wenn h' zur Basis genommen wird, so ist $tt' \equiv 1 \pmod{p-1}$; und wenn unter denselben Voraussetzungen die Indices irgend einer andern Zahl in diesen beiden Systemen respective u und u' sind, so ist $tu' \equiv u$, $t'u \equiv u' \pmod{p-1}$.

IV. Wenn die Zahlen 1, $1+i$ und die drei zu ihnen associierten (als zu trivial) von den von uns zu betrachtenden Moduln ausgeschlossen werden, so bleiben diejenigen Primzahlen übrig, welche wir im Artikel 34 unter 3. und 4. angeführt haben. Die Normen der letzteren sind reelle Primzahlen von der Form $4n+1$, die Normen der ersteren aber Quadrate von ungeraden reellen Primzahlen; in beiden Fällen ist daher $p-1$ durch 4 teilbar.

V. Bezeichnet man den Index der Zahl -1 mit u, so ist $2u \equiv 0 \pmod{p-1}$ und daher entweder $u \equiv 0$ oder $u \equiv \frac{1}{2}(p-1)$. Da aber der Index 0 dem Reste $+1$ entspricht, so muss der Index der Zahl -1 notwendig $\frac{1}{2}(p-1)$ sein.

VI. Bezeichnet man ebenso mit u den Index der Zahl i, so wird $2u \equiv \frac{1}{2}(p-1) \pmod{p-1}$ und daher entweder $u \equiv \frac{1}{4}(p-1)$ oder $u \equiv \frac{3}{4}(p-1)$. Diese Zweideutigkeit hängt aber von der Wahl der primitiven Wurzeln ab. Ist nämlich für die als Basis genommene primitive Wurzel h der Index der Zahl i gleich $\frac{1}{4}(p-1)$, so wird der Index $\frac{3}{4}(p-1)$ werden, wenn h^{μ} zur Basis genommen wird, wo μ eine positive zu $p-1$ prime ganze Zahl von der Form $4n+3$, z. B. die Zahl $p-2$ selbst, bezeichnet und umgekehrt. Daher liefert die eine Hälfte der primitiven Wurzeln für die Zahl i den Index $\frac{1}{4}(p-1)$, die andere den Index $\frac{3}{4}(p-1)$, und offenbar wird für jene Grundzahlen $-i$ den Index $\frac{3}{4}(p-1)$, für diese aber den Index $\frac{1}{4}(p-1)$ besitzen.

VII. Ist der Modul eine positive reelle Primzahl von der Form $4n+3$, etwa gleich q, und daher $p=q^2$, so werden die Indices aller reellen Zahlen durch $q+1$ teilbar sein. Denn bezeichnet t den Index der reellen Zahl k, so ist wegen $k^{q-1} \equiv 1 \pmod{q}$: $(q-1)t \equiv 0 \pmod{q^2-1}$ und daher $\frac{t}{q+1}$ eine ganze Zahl. Ebenso sind die Indices der rein imaginären Zahlen wie ki durch $\frac{1}{2}(q+1)$ teilbar. Es ist somit ersichtlich, dass die primitiven Wurzeln für solche Moduln nur unter den gemischt imaginären Zahlen zu suchen sind.

VIII. Dagegen können für einen Modul m, welcher eine gemischte complexe Primzahl ist (deren Norm somit eine reelle Primzahl von der Form $4n+1$ ist), beliebige primitive Wurzeln auch unter den reellen Zahlen ausgewählt werden, unter denen man sogar ein vollständiges System incongruenter Reste nachweisen kann (Artikel 40). Offenbar aber ist jede reelle Zahl, welche für den complexen Modul m primitive Wurzel ist, zugleich auch in der Arithmetik der reellen Zahlen eine primitive Wurzel für den Modul p und umgekehrt.

56.

Obwohl die Theorie der quadratischen Reste und Nichtreste in der Arithmetik der complexen Zahlen unter der Theorie der

biquadratischen Reste enthalten ist, werden wir doch, bevor wir zu dieser übergehen, die Hauptsätze jener hier besonders vortragen; der Kürze wegen werden wir aber hier nur über den Hauptfall reden, wo der Modul eine complexe (ungerade) Primzahl ist.

Es sei m ein solcher Modul und p seine Norm. Offenbar kann jede ganze (durch m nicht teilbare, wie hier immer hinzuzudenken ist) Zahl einem Quadrate nach dem Modul m entweder congruent werden oder nicht, je nachdem ihr Index, nachdem irgend eine primitive Wurzel zur Basis genommen ist, gerade oder ungerade ist; im ersteren Falle wird jene ganze Zahl quadratischer Rest, im letzteren quadratischer Nichtrest von m genannt. Hieraus folgt, dass unter den $p-1$ Zahlen, welche ein vollständiges System incongruenter (durch m nicht teilbarer) Reste darstellen, die eine Hälfte zu den quadratischen Resten, die andere Hälfte zu den quadratischen Nichtresten gehört. Jeder andern nicht in jenem System vorkommenden Zahl aber ist in dieser Hinsicht derselbe Character beizulegen, welchen die ihr congruente Zahl des Systems besitzt.

Ferner folgt ebendaraus, dass das Product aus zwei quadratischen Resten ebenso wie das Product aus zwei quadratischen Nichtresten quadratischer Rest ist, dagegen das Product aus einem quadratischen Reste und einem quadratischen Nichtreste ein Nichtrest wird; und allgemein, dass das Product aus beliebig vielen Factoren quadratischer Rest oder Nichtrest ist, je nachdem die Anzahl der Nichtreste unter jenen Factoren gerade oder ungerade ist.

Um die quadratischen Reste von den quadratischen Nichtresten zu unterscheiden, hat man sogleich das folgende allgemeine Kriterium:

Die durch den Modul nicht teilbare Zahl k ist quadratischer Rest oder Nichtrest desselben, je nachdem man entweder $k^{\frac{1}{2}(p-1)} \equiv 1$ oder $k^{\frac{1}{2}(p-1)} \equiv -1$ (mod. m) hat.

Die Richtigkeit dieses Satzes folgt sogleich daraus, dass, nachdem eine beliebige primitive Wurzel zur Basis genommen ist, der Index der Potenz $k^{\frac{1}{2}(p-1)}$ entweder $\equiv 0$ oder $\equiv \frac{1}{2}(p-1)$ wird, je nachdem der Index der Zahl k gerade oder ungerade ist.

57.

Es ist zwar leicht, für einen gegebenen Modul das vollständige System incongruenter Reste in zwei Klassen, nämlich in quadratische Reste und Nichtreste, zu teilen, wodurch auch zugleich für alle übrigen Zahlen die ihnen zugehörige Klasse bestimmt wird; bei Weitem schwieriger aber ist die Frage nach den Kriterien, durch welche man diejenigen Moduln, für welche eine gegebene Zahl quadratischer Rest ist, von denen, für welche sie Nichtrest ist, unterscheiden kann.

Was die reellen Einheiten $+1$ und -1 betrifft, so sind diese in der Arithmetik der complexen Zahlen selbst Quadrate und daher auch quadratische Reste für jeden Modul. Ebenso leicht folgt aus dem Kriterium des

vorigen Paragraphen, dass die Zahl i (und ebenso $-i$) quadratischer Rest jedes Moduls ist, dessen Norm p von der Form $8n+1$, dagegen quadratischer Nichtrest jedes Moduls, dessen Norm von der Form $8n+5$ ist. Da es offenbar gleichgiltig ist, ob die Zahl m oder eine der zu ihr associierten Zahlen im, $-m$, $-im$ zum Modul genommen wird, so wird man annehmen dürfen, dass der Modul die primäre Zahl (Artikel 36, II) unter den associierten und somit, wenn man den Modul gleich $a+bi$ setzt, a ungerade, b gerade sei. Da hiernach immer $a^2 \equiv 1 \pmod{8}$, b^2 aber entweder $\equiv 0$ oder $\equiv 4 \pmod{8}$ ist, je nachdem b gerademal gerade oder ungerademal gerade ist, so werden offenbar die Zahlen $+i$ und $-i$ im ersten Falle quadratische Reste, im zweiten quadratische Nichtreste des Moduls sein.

58.

Da die Entscheidung über den Character einer zusammengesetzten Zahl, ob sie quadratischer Rest oder Nichtrest ist, von den Characteren der Factoren abhängt, so genügt es offenbar, wenn wir die Entwicklung von Kriterien zur Unterscheidung derjenigen Moduln, für welche eine gegebene Zahl k quadratischer Rest ist, von denen, für welche sie Nichtrest ist, auf solche Werte von k beschränken, welche Primzahlen und überdies unter den zu ihnen associierten Zahlen die primären sind. Bei dieser Untersuchung liefert uns die Induction sofort sehr elegante Sätze.

Beginnen wir mit der Zahl $1+i$, so finden wir, dass dieselbe quadratischer Rest der Moduln

$$-1+2i,\ +3-2i,\ -5-2i,\ -1-6i,\ +5+4i,\ +5-4i,\ -7,$$
$$+7+2i,\ -5+6i, \ldots,$$

dagegen quadratischer Nichtrest der folgenden Moduln ist:

$$-1-2i,\ -3,\ +3+2i,\ +1+4i,\ +1-4i,\ -5+2i,\ -1+6i,$$
$$+7-2i,\ -5-6i,\ -3+8i,\ -3-8i,\ +5+8i,\ +5-8i,$$
$$+9+4i,\ +9-4i, \ldots$$

Wenn wir diese Übersicht, in welche wir von je vier associierten Moduln immer den primären aufgenommen haben, aufmerksam betrachten, so bemerken wir leicht, dass die Moduln $a+bi$ in der ersteren Klasse sämtlich so beschaffen sind, dass für sie $a+b \equiv +1 \pmod{8}$, die in der letzteren Klasse aber so, das für sie $a+b \equiv -3 \pmod{8}$ ist. Offenbar muss dieses Kriterium, wenn wir an Stelle des primären Moduls m den associierten $-m$ nehmen, derart abgeändert werden, dass für Moduln der ersten Klasse $a+b \equiv -1$, für Moduln der letzten Klasse aber $a+b \equiv +3 \pmod{8}$ ist. Daher wird allgemein, wenn anders uns die Induction nicht getäuscht hat, und wenn $a+bi$ eine Primzahl bezeichnet, in welcher a ungerade, b gerade ist, $1+i$ quadratischer Rest oder Nichtrest derselben sein, je nachdem $a+b \equiv \pm 1$ oder $\equiv \pm 3 \pmod{8}$ ist.

Für die Zahl $-1-i$ gilt dieselbe Regel, wie für $1+i$. Betrachtet man andererseits $1-i$ als Product aus $-i$ und $1+i$, so ist klar, dass der Zahl $1-i$ derselbe Character zukommt, welcher $1+i$ beizulegen ist, wenn b gerademal gerade, dagegen der entgegengesetzte, wenn b ungerademal gerade ist, woraus leicht folgt, dass $1-i$ quadratischer Rest der Primzahl $a+bi$ ist, wenn $a-b\equiv\pm 1$ ist, quadratischer Nichtrest aber, wenn $a-b\equiv\pm 3$ (mod. 8) ist, immer unter der Voraussetzung, dass a ungerade, b gerade ist.

Übrigens kann dieser zweite Satz aus dem ersten auch abgeleitet werden mit Hülfe eines allgemeineren **Satzes**, welchen wir folgendermassen aussprechen:

In der Theorie der quadratischen Reste ist der Character der Zahl $\alpha+\beta i$ in Bezug auf den Modul $a+bi$ derselbe, wie der Character der Zahl $\alpha-\beta i$ in Bezug auf den Modul $a-bi$.

Der Beweis dieses Satzes ergiebt sich daraus, dass beide Moduln dieselbe Norm p haben und dass, sooft $(\alpha+\beta i)^{\frac{1}{2}(p-1)}-1$ durch $a+bi$ teilbar ist, auch $(\alpha-\beta i)^{\frac{1}{2}(p-1)}-1$ durch $a-bi$ teilbar ist, sooft aber $(\alpha+\beta i)^{\frac{1}{2}(p-1)}+1$ durch $a+bi$ geteilt werden kann, auch $(\alpha-\beta i)^{\frac{1}{2}(p-1)}+1$ durch $a-bi$ teilbar sein muss.

59.

Wir gehen nun weiter zu ungeraden Primzahlen.

Wir finden, dass die Zahl $-1+2i$

quadratischer Rest ist der Moduln:

$+3+2i,\ +1-4i,\ -5+2i,\ -5-2i,\ -1-6i,\ +7-2i,\ -3+8i,$
$+5+8i,\ +5-8i,\ +9+4i,\ \ldots,$

quadratischer Nichtrest aber der Moduln:

$-1-2i,\ -3,\ +3-2i,\ +1+4i,\ -1+6i,\ +5+4i,\ +5-4i,\ -7,$
$+7+2i,\ -5+6i,\ -5-6i,\ -3-8i,\ +9-4i,\ \ldots$

Reduciert man die Moduln der ersten Klasse auf ihre absolut kleinsten Reste nach dem Modul $-1+2i$, so findet man nur die folgenden $+1$ und -1, nämlich $+3+2i\equiv-1$, $+1-4i\equiv-1$, $-5+2i\equiv+1$, $-5-2i\equiv-1$, u. s. w.

Andererseits findet man, dass sämtliche Moduln der letzteren Klasse nach dem Modul $-1+2i$ entweder $\equiv+i$ oder $\equiv-i$ sind.

Nun sind aber $+1$ und -1 selbst quadratische Reste des Moduls $-1+2i$ und $+i$ und $-i$ quadratische Nichtreste desselben. Mithin ergiebt sich, soweit man der Induction Glauben schenken darf, der folgende **Satz:**

Die Zahl $-1+2i$ ist quadratischer Rest oder Nichtrest einer Primzahl $a+bi$, je nachdem diese quadratischer Rest oder Nichtrest von $-1+2i$

ist, wofern nämlich $a + bi$ unter den vier associierten Zahlen die primäre oder vielmehr, wenn a ungerade, b gerade ist.

Ferner folgen aus diesem Satze ohne Weiteres die analogen Sätze bezüglich der Zahlen $+1-2i$, $-1-2i$, $+1+2i$.

60.

Stellt man eine ähnliche Induction bezüglich der Zahl -3 oder $+3$ an, so findet man, dass jede der beiden

quadratischer Rest ist der Moduln:

$$+3+2i,\ +3-2i,\ -1+6i,\ -1-6i,\ -7,\ -5+6i,\ -5-6i,\ -3+8i,\ -3-8i,\ +9+4i,\ +9-4i,\ \ldots$$

aber quadratischer Nichtrest der Moduln:

$$-1+2i,\ -1-2i,\ +1+4i,\ +1-4i,\ -5+2i,\ -5-2i,\ +5+4i,\ +5-4i,\ +7+2i,\ +7-2i,\ +5+8i,\ +5-8i,\ \ldots.$$

Die ersteren sind nach dem Modul 3 irgend einer von den vier Zahlen $+1$, -1, $+i$, $-i$, die letzteren aber einer von den vier folgenden $+1+i$, $+1-i$, $-1+i$, $-1-i$ congruent. Jene sind selbst quadratische Reste, diese quadratische Nichtreste von 3.

Es lehrt daher diese Induction, dass die Primzahl $a + bi$, immer vorausgesetzt, dass a ungerade, b gerade sei, zur Zahl -3 (sowie zu $+3$) dieselbe Relation hat, wie diese zu jener, insoweit nämlich die eine quadratischer Rest oder Nichtrest der andern ist.

Dehnt man diese Induction auf andere Primzahlen aus, so findet man überall dieses höchst elegante Reciprocitätsgesetz bestätigt und gelangt so zu dem folgenden **Fundamentaltheorem** bezüglich der quadratischen Reste in der Arithmetik der complexen Zahlen:

Bezeichnen $a + bi$, $A + Bi$ Primzahlen von der Beschaffenheit, dass a, A ungerade, b, B gerade sind, so wird entweder jede der beiden quadratischer Rest oder jede der beiden quadratischer Nichtrest der andern sein.

Trotz der grossen Einfachheit des Satzes aber unterliegt sein Beweis sehr grossen Schwierigkeiten, mit denen wir uns jedoch hier nicht aufhalten, da der Satz selbst nur ein specieller Fall eines allgemeineren Satzes ist, welcher die ganze Theorie der biquadratischen Reste in sich enthält. Zu dieser wollen wir daher jetzt übergehen.

61.

Was im Artikel 2 der früheren Abhandlung über den Begriff des biquadratischen Restes und Nichtrestes angeführt worden ist, dehnen wir auch auf die Arithmetik der complexen Grössen aus und beschränken ebenso

wie dort auch hier die Untersuchung auf solche Moduln, welche Primzahlen sind; zugleich wird man sich meistens, ohne dass darauf hingewiesen wird, hinzudenken müssen, dass der Modul derart angenommen wird, dass er unter den associierten Zahlen der primäre, nämlich $\equiv 1$ nach dem Modul $2+2i$ ist, sowie ferner, dass die Zahlen, um deren Character (insofern sie biquadratische Reste oder Nichtreste sind) es sich handelt, durch den Modul nicht teilbar sind.

Für einen gegebenen Modul also könnten die durch ihn nicht teilbaren Zahlen in drei Klassen eingeteilt werden, von denen die erste die biquadratischen Reste, die zweite diejenigen biquadratischen Nichtreste, welche quadratische Reste sind, die dritte endlich die quadratischen Nichtreste enthielte. Aber auch hier ist es vorteilhafter, an Stelle der dritten Klasse zwei aufzustellen, so dass man im Ganzen vier Klassen hat.

Hat man irgend eine primitive Wurzel zur Basis genommen, so werden die biquadratischen Reste Indices haben, die durch 4 teilbar oder von der Form $4n$ sind; diejenigen Nichtreste, welche quadratische Reste sind, werden Indices haben von der Form $4n+2$; endlich werden die Indices der quadratischen Nichtreste zum Teil von der Form $4n+1$ zum Teil von der Form $4n+3$ sein. Auf diese Weise würden allerdings vier Klassen entstehen; indessen würde der Unterschied zwischen den beiden letzten Klassen kein absoluter, sondern von der Wahl der zur Basis genommenen primitiven Wurzel abhängig sein; denn man sieht leicht, dass für die eine Hälfte der primitiven Wurzeln ein gegebener quadratischer Nichtrest einen Index von der Form $4n+1$, für die andere Hälfte aber einen Index von der Form $4n+3$ erhält. Um diese Zweideutigkeit zu beseitigen, werden wir annehmen, dass stets eine solche primitive Wurzel gewählt wird, für welche der Index $\frac{1}{4}(p-1)$ zur Zahl $+i$ gehört (vgl. Artikel 55, VI). Auf diese Weise entsteht eine Klasseneinteilung, die wir kürzer unabhängig von den primitiven Wurzeln in folgender Weise darstellen können:

Die erste Klasse möge diejenigen Zahlen k enthalten, für welche $k^{\frac{1}{4}(p-1)} \equiv 1$ wird; diese Zahlen sind die biquadratischen Reste des Moduls.

Die zweite Klasse möge diejenigen Zahlen enthalten, für welche $k^{\frac{1}{4}(p-1)} \equiv i$ wird.

Die dritte Klasse möge diejenigen Zahlen enthalten, für welche $k^{\frac{1}{4}(p-1)} \equiv -1$ wird.

Die vierte Klasse endlich möge diejenigen Zahlen enthalten, für welche $k^{\frac{1}{4}(p-1)} \equiv -i$ wird.

Die dritte Klasse wird diejenigen biquadratischen Nichtreste enthalten, welche quadratische Reste sind; in die zweite und vierte Klasse teilen sich die quadratischen Nichtreste.

Den Zahlen dieser Klassen werden wir respective den **biquadratischen Character** 0, 1, 2, 3 beilegen. Wenn wir den Character λ einer Zahl k nach dem Modul m so definieren, dass er der Exponent derjenigen Potenz von i

sein soll, welcher die Zahl $k^{\frac{1}{4}(p-1)}$ congruent ist, so sind offenbar die nach dem Modul 4 congruenten Charactere als äquivalent zu betrachten. Übrigens wird dieser Begriff vorerst auf diejenigen Moduln, welche Primzahlen sind, beschränkt; in der Fortsetzung dieser Untersuchungen werden wir zeigen, wie er auch zusammengesetzten Moduln angepasst werden kann.

62.

Damit wir um so leichter eine ausführliche Induction hinsichtlich der Charactere der Moduln anstellen können, fügen wir hier eine umfangreiche **Tafel** hinzu, mit deren Hülfe der Character einer jeden gegebenen Zahl in Bezug auf einen Modul, dessen Norm den Wert 157 nicht übersteigt, mit geringer Mühe erhalten wird, wofern man nur auf folgende Bemerkungen achtet.

Da der Character einer zusammengesetzten Zahl gleich (oder nach dem Modul 4 congruent) ist dem Aggregat der Charactere der einzelnen Factoren, so genügt es, wenn wir für einen gegebenen Modul die Charactere der Primzahlen bestimmen können. Da ferner die Charactere der Einheiten -1, $+i$, $-i$ offenbar den Zahlen $\frac{1}{2}(p-1)$, $\frac{1}{4}(p-1)$, $\frac{3}{4}(p-1)$ nach dem Modul 4 congruent sind, so wird es auch ausreichen, wenn nur die Charactere der primären Zahlen unter den associierten dargestellt werden. Da endlich die nach dem Modul m congruenten Zahlen denselben Character haben, so genügt es, die Charactere solcher Zahlen in die Tafel aufzunehmen, welche in dem System der absolut kleinsten Reste enthalten sind. Ausserdem beweist man durch eine ähnliche Schlussreihe wie im Artikel 58, dass, wenn für den Modul $a+bi$ der Character der Zahl $A+Bi$ gleich λ, für den Modul $a-bi$ aber λ' der Character der Zahl $A-Bi$ ist, immer $\lambda \equiv -\lambda' \pmod{4}$ oder $\lambda+\lambda'$ durch 4 teilbar ist; mithin braucht man nur Moduln in die Tafel aufzunehmen, in welchen b entweder gleich 0 oder positiv ist.

Wenn z. B. der Character der Zahl $11-6i$ in Bezug auf den Modul $-5-6i$ gesucht wird, so substituieren wir für diese Zahlen die folgenden $11+6i$, $-5+6i$; sodann bestimmen wir (Artikel 43) den absolut kleinsten Rest der Zahl $11+6i$ nach dem Modul $-5+6i$, welcher $-1-4i = -1 \times (1+4i)$ wird. Mithin ist, da für den Modul $-5+6i$ der Character von -1 gleich 30, der Character der Zahl $1+4i$ aber nach der Tafel 2 ist, 32 oder 0 der Character der Zahl $11+6i$ für den Modul $-5+6i$ und somit nach der letzten Bemerkung auch der Character der Zahl $11-6i$ für den Modul $-5-6i$. — Ebenso zerlegt man, wenn der Character der Zahl $-5+6i$ in Bezug auf den Modul $11+6i$ gesucht wird, den absolut kleinsten Rest jener $1-5i$ in die Factoren $-i$, $1+i$, $3-2i$, denen die Charactere 117, 0, 1 entsprechen, so dass der gesuchte Character 118 oder 2 ist; ebenderselbe Character ist auch der Zahl $-5-6i$ in Bezug auf den Modul $11-6i$ beizulegen.

Modul	Character	Zahlen
-3	3	$1+i$
$+3+2i$	3	$1+i$
$+1+4i$	1	$-1+2i$
	3	$1+i$
$-5+2i$	0	$-1-2i$
	1	$1+i$
	2	$-1+2i$
$-1+6i$	0	-3
	1	$1+i,\ -1+2i$
	2	$-1-2i$
$+5+4i$	0	$1+i$
	1	-3
	3	$-1+2i,\ -1-2i$
-7	0	-3
	1	$-1+2i,\ 3-2i$
	2	$1+i$
	3	$-1-2i,\ 3+2i$
$+7+2i$	0	$1+i,\ 3+2i,\ 3-2i,\ 1-4i$
	1	-3
	2	$-1-2i,\ 1+4i$
	3	$-1+2i$
$-5+6i$	0	$1+i,\ -3,\ 3+2i,\ 3-2i$
	1	$1-4i$
	2	$1+4i$
	3	$-1+2i,\ -1-2i$
$-3+8i$	0	$-1+2i,\ 3-2i,\ 1-4i$
	1	$1+i,\ 3+2i$
	2	-3
	3	$-1-2i,\ 1+4i,\ -5+2i$
$+5+8i$	0	$-1-2i$
	1	$-5-2i,\ -1+6i$
	2	$-1+2i,\ 3-2i$
	3	$1+i,\ -3,\ 3+2i,\ 1+4i,\ 1-4i$
$+9+4i$	0	$-1+2i,\ 3+2i$
	1	$1+i,\ -1-2i,\ 3-2i$
	2	$-3,\ 1+4i$
	3	$1-4i,\ -5+2i$
$-1+10i$	0	$1+i,\ -1+2i,\ -1-2i,\ 3+2i$
	1	-3
	2	$3-2i,\ -5+2i,\ 5-4i$
	3	$1+4i,\ 1-4i$
$+3+10i$	1	$1+i,\ -1-2i,\ 1-4i$

Modul	Character	Zahlen
$+3+10i$	2	$-3,\ 3+2i,\ 1+4i,\ -5-2i$
	3	$-1+2i,\ 3-2i$
$-7+8i$	0	$1+i,\ -7$
	1	$3+2i,\ 3-2i,\ 1-4i,\ -5-2i$
	2	$-1-2i,\ 1+4i,\ -5+2i,\ -1-6i$
	3	$-1+2i,\ -3,\ -1+6i$
-11	0	-3
	1	$1+i,\ 3-2i,\ 1+4i,\ -5+2i,\ 5+4i$
	2	$-1+2i,\ -1-2i$
	3	$3+2i,\ 1-4i,\ -5-2i,\ 5-4i$
$-11+4i$	0	$1+i,\ -1+2i,\ 3+2i,\ 5+4i$
	1	$-1-2i,\ -1+6i$
	2	$-5+2i$
	3	$-3,\ 3-2i,\ 1+4i,\ 1-4i,\ -5-2i$
$+7+10i$	0	$1+4i,\ 1-4i,\ -1+6i,\ -1-6i$
	1	$-1+2i,\ 3+2i,\ -5+2i$
	2	$1+i,\ 3-2i$
	3	$-1-2i,\ -3,\ -5-2i$
$+11+6i$	0	$1+i,\ -1+2i,\ -3,\ 1+4i,\ 1-4i,\ -7$
	1	$-1-2i,\ 3+2i,\ 3-2i$
	2	$-5-2i,\ -1+6i,\ 5-4i$
	3	$-5+2i,\ 5+4i,\ 7-2i.$

63.

Wir wollen nun versuchen, die gemeinschaftlichen Kriterien der Moduln, für welche eine gegebene Primzahl denselben Character hat, durch Induction zu entdecken. Wir setzen stets voraus, dass die Moduln unter den associirten Zahlen primär seien, also solche Moduln $a+bi$, für welche entweder $a\equiv 1,\ b\equiv 0$ oder $a\equiv 3,\ b\equiv 2$ (mod. 4) ist.

In Bezug auf die Zahl $1+i$, mit welcher wir den Anfang machen, stösst man leichter auf das Inductionsgesetz, wenn man die Moduln der ersteren Art (für welche $a\equiv 1,\ b\equiv 0$) von den Moduln der letzteren Art (für welche $a\equiv 3,\ b\equiv 2$) trennt. Mit Hülfe der Tafel des vorigen Artikels findet man, dass entspricht

der Character	den Moduln der ersteren Art:
0	$5+4i,\ -7+8i,\ -7-8i,\ -11+4i$
1	$1-4i,\ -3+8i,\ -3-8i,\ 9+4i,\ -11$
2	$5-4i,\ -7,\ -11-4i$
3	$-3,\ 1+4i,\ 5+8i,\ 5-8i,\ 9-4i.$

Wenn wir diese sechzehn Beispiele mit Aufmerksamkeit betrachten, so finden wir in allen den Character $\equiv \frac{1}{4}(a-b-1)$ (mod. 4).

Ebenso entspricht

der Character	den Moduln der zweiten Art
0	$3-2i,\ -1-6i,\ 7+2i,\ -5+6i,\ -1+10i,\ 11+6i$
1	$-5+2i,\ -1+6i,\ 7-2i,\ -1-10i,\ 3+10i$
2	$-1+2i,\ -5-2i,\ 3-10i,\ 7+10i$
3	$-1-2i,\ 3+2i,\ -5-6i,\ 7-10i,\ 11-6i.$

In allen diesen zwanzig Beispielen findet man bei einiger Aufmerksamkeit den Character $\equiv \frac{1}{4}(a-b-5)$ (mod. 4).

Diese beiden Regeln kann man leicht in eine für jede der beiden Arten von Moduln geltende zusammenziehen, wenn man erwägt, dass $\frac{1}{4}b^2$ für Moduln der ersten Art $\equiv 0$, für Moduln der zweiten Art $\equiv 1$ (mod. 4) ist. Es ist daher der Character der Zahl $1+i$ in Bezug auf jeden primen unter den associierten Zahlen primären Modul $\equiv \frac{1}{4}(a-b-1-b^2)$ (mod. 4).

Nebenbei wollen wir hier bemerken, dass, da $(b+1)^2$ immer von der Form $8n+1$ oder $\frac{1}{4}(2b+b^2)$ gerade ist, jener Character stets gerade oder ungerade wird, je nachdem $\frac{1}{4}(a+b-1)$ gerade oder ungerade ist, was mit der für den quadratischen Character im Artikel 58 angegebenen Regel übereinstimmt.

Da $\frac{1}{4}(a-b-1)$, $\frac{1}{4}(a-b+3)$ ganze Zahlen sind, von denen die eine gerade, die andere ungerade ist, so wird das Product derselben gerade oder $\frac{1}{8}(a-b-1)(a-b+3) \equiv 0$ (mod. 4) sein. Hiernach kann an Stelle des angegebenen Ausdrucks für den biquadratischen Character auch der folgende genommen werden:

$$\tfrac{1}{4}(a-b-1-b^2)-\tfrac{1}{8}(a-b-1)(a-b+3)=\tfrac{1}{8}(-a^2+2ab-3b^2+1),$$

welche Form sich auch dadurch empfiehlt, dass sie nicht auf primäre Moduln beschränkt ist, sondern nur voraussetzt, dass a ungerade, b gerade sei; denn offenbar wird unter dieser Voraussetzung entweder $a+bi$ oder $a-bi$ unter den associierten Zahlen die primäre sein, und der Wert jener Formel ist für beide Moduln derselbe.

64.

Gehen wir von der letzten im vorigen Artikel gefundenen Regel aus, so sehen wir, dass

für die Zahl	der Character $\equiv$
$-1+i$	$\frac{1}{8}(a^2+2ab-b^2-1)$
$-1-i$	$\frac{1}{8}(-a^2+2ab+b^2+1)$
$+1-i$	$\frac{1}{8}(a^2+2ab+3b^2-1).$

Dies folgt sogleich daraus, dass der Character von $i\ \frac{1}{4}(a^2 + b^2 - 1)$, der Character von -1 aber $\frac{1}{2}(a^2 + b^2 - 1) \equiv \frac{1}{2}b^2$ ist, da $a^2 - 1$ immer von der Form $8n$ ist. Offenbar sind diese vier Regeln, obwohl sie bisher nur durch Induction erhalten sind, derart mit einander verbunden, dass, sobald der Beweis der einen von ihnen erledigt ist, die drei übrigen zugleich mit bewiesen sind. Es ist kaum nötig, darauf hinzuweisen, dass auch in diesen Regeln nur vorausgesetzt wird, dass a ungerade, b gerade sei.

Wenn man Formeln anwenden will, welche auf primäre Moduln beschränkt sind, so kann man sich folgender Form bedienen. Es ist

für die Zahl	der Character $\equiv$
$-1-i$	$\frac{1}{4}(-a-b+1-b^2)$
$-1-i$	$\frac{1}{4}(\ \ a-b-1+b^2)$
$+1-i$	$\frac{1}{4}(-a-b+1+b^2)$.

Die einfachsten Formeln ergeben sich, wenn wir, wie wir es im Anfange unserer Induction gethan haben, Moduln der ersten und zweiten Art unterscheiden. Es ist nämlich der Character

der Zahl	für Moduln der ersten Art	für Moduln der zweiten Art
$-1+i$	$\frac{1}{4}(-a-b+1)$	$\frac{1}{4}(-a-b-3)$
$-1-i$	$\frac{1}{4}(\ \ a-b-1)$	$\frac{1}{4}(\ \ a-b+3)$
$+1-i$	$\frac{1}{4}(-a-b+1)$	$\frac{1}{4}(-a-b+5)$.

65.

Für die Zahl $-1+2i$, zu welcher wir jetzt übergehen, wollen wir ebenfalls die Unterscheidung zwischen denjenigen Moduln $a+bi$, für welche $a \equiv 1$, $b \equiv 0$, und denjenigen, für welche $a \equiv 3$, $b \equiv 2$ ist, machen. Die Tafel des Artikels 62 zeigt, dass in Bezug auf jene Zahl

der Character	den Moduln erster Art entspricht
0	$-3+8i$, $+5-8i$, $+9+4i$, $-11+4i$
1	$+1+4i$, $+5-4i$, -7, $-3-8i$
2	$+1-4i$, $+5+8i$, $-7-8i$, -11
3	-3, $+5+4i$, $+9-4i$, $-7+8i$, $-11-4i$.

Reducieren wir diese einzelnen Moduln auf die absolut kleinsten Reste nach dem Modul $-1+2i$, so bemerken wir, dass alle, denen der Character 0 entspricht, $\equiv 1$, diejenigen, denen der Character 1 entspricht, $\equiv i$, diejenigen, deren Character 2 ist, $\equiv -1$, endlich diejenigen, deren Character 3 ist, $\equiv -i$ werden. Nun sind aber die Charactere der Zahlen $1, i, -1, -i$ für den Modul $-1+2i$ gerade 0, 1, 2, 3 respective; mithin ist in allen diesen siebzehn Beispielen der Character der Zahl $-1+2i$ in

Bezug auf den Modul erster Art $a+bi$ mit dem Character dieser Zahl in Bezug auf den Modul $-1+2i$ identisch.

Ebenso findet man mit Hülfe der Tafel, dass

der Character	den Moduln zweiter Art entspricht
0	$+3+2i, -5-2i, -1+10i, -1-10i, +11+6i$
1	$+3-2i, -1+6i, -5-6i, +7+10i, +7-10i$
2	$-5+2i, -1-6i, +7-2i$
3	$-1-2i, +7+2i, -5+6i, +3+10i, +3-10i, +11-6i.$

Bringt man diese Moduln auf ihre absolut kleinsten Reste nach dem Modul $-1+2i$, so findet man, dass alle, denen respective die Charactere 0, 1, 2, 3 entsprechen, den Zahlen -1, $-i$, $+1$, $+i$ congruent sind; diesen Zahlen selbst aber kommen, wenn umgekehrt $-1+2i$ znm Modul genommen wird, die Charactere 2, 3, 0, 1 respective zu. Mithin ist in allen diesen neunzehn Beispielen der Character der Zahl $-1+2i$ in Bezug auf einen Modul der zweiten Art um zwei Einheiten von dem Character dieser Zahl in Bezug auf die zum Modul genommene Zahl $-1+2i$ verschieden.

Ferner sieht man leicht, dass ganz Ähnliches in Bezug auf die Zahl $-1-2i$ stattfinden wird.

66.

Für die Zahl -3 unterlassen wir eine Unterscheidung zwischen Moduln erster und zweiter Art, da der Erfolg lehrt, dass eine solche hier überflüssig ist. Es entspricht daher

der Character	den Moduln
0	$-1+6i, -1-6i, -7, -5+6i, -5-6i, -11, 11+6i, 11-6i$
1	$-1-2i,\ 1-4i,\ -5+2i,\ 5+4i,\ 7+2i,\ 5-8i,\ -1+10i,$ $-7-8i,\ -11-4i,\ 7-10i$
2	$3+2i,\ 3-2i,\ -3+8i,\ -3-8i,\ 9+4i,\ 3+10i,\ 3-10i$
3	$-1+2i,\ 1+4i,\ -5-2i,\ 5-4i,\ 7-2i,\ 5+8i,\ -1-10i,$ $-7+8i,\ -11+4i,\ 7+10i.$

Bringen wir diese Moduln auf ihre kleinsten Reste nach dem Modul 3, so sehen wir, dass diejenigen, welchen der Character 0 entspricht, zum Teil $\equiv 1$, zum Teil $\equiv -1$, diejenigen, deren Character 1 ist, entweder $\equiv 1-i$ oder $\equiv -1+i$, diejenigen, deren Character 2 ist, entweder $\equiv i$ oder $\equiv -i$, endlich diejenigen, denen der Character 3 zukommt, entweder $\equiv 1+i$ oder $\equiv -1-i$ sind. Aus dieser Induction schliessen wir daher, dass der Character der Zahl -3 für einen primen unter den associierten Zahlen primären Modul identisch ist mit dem Character dieses Moduls, wenn 3 oder, was auf dasselbe hinauskommt, -3 als Modul betrachtet wird.

67.

Stellt man in Bezug auf andere Primzahlen eine ähnliche Induction an, so findet man, dass die Zahlen $3 \pm 2i$, $-1 \pm 6i$, $7 \pm 2i$, $-5 \pm 6i$, ... ähnliche Sätze liefern, wie derjenige ist, zu welchem wir im Artikel 65 in Bezug auf die Zahl $-1 + 2i$ gelangt sind, dass dagegen die Zahlen $1 \pm 4i$, $5 \pm 4i$, $-3 \pm 8i$, $5 \pm 8i$, $9 \pm 4i$, ... sich ebenso verhalten, wie die Zahl -3. Die Induction führt also zu einem sehr eleganten Satze, den man, nach Analogie der Theorie der quadratischen Reste in der Arithmetik der reellen Zahlen, das **Fundamentaltheorem** der biquadratischen Reste nennen kann, nämlich:

Bezeichnen $a + bi$, $a' + b'i$ zwei verschiedene, unter den zu ihnen associierten Zahlen primäre, d. h. nach dem Modul $2 + 2i$ der Einheit congruente Primzahlen, so ist der biquadratische Character der Zahl $a + bi$ in Bezug auf den Modul $a' + b'i$ identisch mit dem Character der Zahl $a' + b'i$ in Bezug auf den Modul $a + bi$, wenn entweder jede oder wenigstens eine der beiden Zahlen $a + bi$, $a' + b'i$ zur ersten Art gehört d. h. nach dem Modul 4 der Einheit congruent ist; dagegen werden jene Charactere um zwei Einheiten verschieden sein, wenn keine der beiden Zahlen $a + bi$, $a' + b'i$ zur ersten Art gehört, d. h. wenn beide nach dem Modul 4 der Zahl $3 + 2i$ congruent sind.

Trotz der grossen Einfachheit dieses Satzes aber gehört doch der Beweis desselben zu den verborgensten Geheimnissen der höheren Arithmetik, so dass er, wenigstens wie jetzt die Sachen liegen, nur mittelst der subtilsten Untersuchungen, welche die Grenzen dieser Abhandlung weit überschreiten würden, geführt werden kann. Daher behalten wir uns die Veröffentlichung dieses Beweises sowie die Entwicklung des Zusammenhanges zwischen diesem Satze und denjenigen, welche wir am Anfange dieser Abhandlung durch Induction festzustellen begonnen haben, für eine dritte Abhandlung vor. Zum Schlusse wollen wir jedoch schon hier angeben, was zum Beweise der in den Artikeln 63 und 64 aufgestellten Sätze erforderlich ist.

68.

Wir beginnen mit solchen Primzahlen $a + bi$, für welche $b = 0$ ist (von der dritten Art des Artikels 34), wo somit (damit die Zahl unter den associierten primär sei) a eine reelle negative Primzahl von der Form $-(4n + 3)$ sein muss, für welche wir $-q$ schreiben werden. Solcher Art sind die Zahlen -3, -7, -11, -19, ... Bezeichnet man λ den Character der Zahl $1 + i$, wenn jene Zahl zum Modul genommen wird, so muss sein:

$$i^\lambda \equiv (1 + i)^{\frac{1}{4}(q^2-1)} \equiv 2^{\frac{1}{8}(q^2-1)} \cdot i^{\frac{1}{8}(q^2-1)} \pmod{q}.$$

Bekanntlich aber ist 2 quadratischer Rest oder Nichtrest von q, je nachdem

q von der Form $8n+7$ oder von der Form $8n+3$ ist, woraus folgt, dass allgemein

$$2^{\frac{1}{2}(q-1)} \equiv (-1)^{\frac{1}{4}(q+1)} \equiv i^{\frac{1}{2}(q+1)} \pmod{q}$$

und somit, wenn man zur Potenz mit dem Exponenten $\frac{1}{4}(q+1)$ erhebt,

$$2^{\frac{1}{8}(q^2-1)} \equiv i^{\frac{1}{8}(q+1)^2} \pmod{q}$$

ist. Daher nimmt die vorhergehende Gleichung die folgende Form an:

$$i^{\lambda} \equiv i^{\frac{1}{8}(q+1)^2+\frac{1}{8}(q^2-1)} \equiv i^{\frac{1}{4}(q^2+q)} \pmod{q},$$

und hieraus folgt:

$$\lambda \equiv \tfrac{1}{4}(q^2+q) \equiv \tfrac{1}{4}(q+1)^2 - \tfrac{1}{4}(q+1) \pmod{4}$$

oder, da man $\frac{1}{4}(q+1)^2 \equiv 0 \pmod{4}$ hat:

$$\lambda \equiv -\tfrac{1}{4}(q+1) \equiv \tfrac{1}{4}(a-1) \pmod{4}.$$

Dies ist der Satz des Artikels 63 für den Fall $b=0$.

69.

Bei weitem schwieriger aber lassen sich solche Moduln $a+bi$ erledigen, für welche b nicht gleich Null ist (die Zahlen der vierten Art des Artikels 34), und müssen erst mehrere Untersuchungen vorausgeschickt werden. Die Norm a^2+b^2, welche eine reelle Primzahl von der Form $4n+1$ ist, bezeichnen wir mit p.

Es möge mit S der Complex aller einfach kleinsten Reste für den Modul $a+bi=m$ mit Ausschluss der Null bezeichnet werden, so dass die Anzahl der in S enthaltenen Zahlen gleich $p-1$ ist. Es bezeichne ferner $x+yi$ unbestimmt irgend eine Zahl dieses Systems, und man setze $ax+by=\xi$, $ay-bx=\eta$. Es sind daher ξ und η ganze Zahlen, welche zwischen den Grenzen 0 und p, diese Grenzen ausgeschlossen, enthalten sind; denn im vorliegenden Falle, wo a und b prim zu einander sind, zeigen die Formeln des Artikels 45, nämlich $\eta \equiv k\xi$, $\xi \equiv -k\eta \pmod{p}$, dass keine der Zahlen ξ, η gleich 0 sein kann, wenn nicht die andere gleichzeitig verschwindet und somit $x=0$, $y=0$ wird, eine Combination, die wir bereits ausgeschlossen haben. Das Kriterium dafür also, dass die Zahl $x+yi$ in S enthalten sei, besteht darin, dass die vier Zahlen ξ, η, $p-\xi$, $p-\eta$ positiv sein müssen.

Ferner bemerken wir, dass für keine solche Zahl $\xi=\eta$ sein kann, denn hieraus würde folgen $p(x+y)=a(\xi+\eta)+b(\xi-\eta)=2a\xi$, was absurd ist, da keiner der Factoren 2, a, ξ durch p teilbar ist. Auf ähnliche Weise lehrt die Gleichung $p(x-y+a+b)=2a\xi+(a+b)(p-\xi-\eta)$, dass $\xi+\eta$ nicht gleich p sein kann. Daher erhalten wir hieraus, da

$\xi - \eta$, $p - \xi - \eta$ entweder positiv oder negativ sein müssen, eine Einteilung des Systems S in vier Complexe C, C', C'', C''' und zwar in der Weise, dass wir setzen

in den Complex	die Zahlen, für welche
C	$\xi - \eta$ positiv, $p - \xi - \eta$ positiv
C'	$\xi - \eta$ positiv, $p - \xi - \eta$ negativ
C''	$\xi - \eta$ negativ, $p - \xi - \eta$ negativ
C'''	$\xi - \eta$ negativ, $p - \xi - \eta$ positiv.

Das Kennzeichen einer Zahl des Complexes C ist also eigentlich ein sechsfaches; es müssen nämlich die sechs Zahlen ξ, η, $p - \xi$, $p - \eta$, $\xi - \eta$, $p - \xi - \eta$ positiv sein; offenbar aber enthalten die zweite, fünfte und sechste Bedingung schon von selbst die übrigen in sich. Analoges gilt von den Complexen C', C'', C''', so dass die vollständigen Kriterien dreifach sind, nämlich

für den Complex	müssen positiv sein die Zahlen
C	η, $\xi - \eta$, $p - \xi - \eta$
C'	$p - \xi$, $\xi - \eta$, $\xi + \eta - p$
C''	$p - \eta$, $\eta - \xi$, $\xi + \eta - p$
C'''	ξ, $\eta - \xi$, $p - \xi - \eta$.

Ferner wird jeder, auch ohne dass wir darauf hinweisen, einsehen, dass bei der geometrischen Darstellung der complexen Zahlen (vgl. Artikel 39) die Zahlen des Systems S innerhalb eines Quadrates enthalten sind, dessen Seiten die Punkte verbinden, durch welche die Zahlen 0, $a + bi$, $(1 + i)(a + bi)$, $i(a + bi)$ dargestellt werden, und dass die Einteilung des Systems S der Teilung des Quadrats durch seine Diagonalen entspricht. Doch wollten wir uns hier lieber rein arithmetischer Schlüsse bedienen, indem wir der Kürze halber die Illustration durch eine bildliche Darstellung dem erfahrenen Leser überlassen.

70.

Wenn die vier complexen Zahlen

$$r = x + yi, \quad r' = x' + y'i, \quad r'' = x'' + y''i, \quad r''' = x''' + y'''i$$

derart mit einander verbunden sind, dass man

$$r' = m + ir, \quad r'' = m + ir' = (1 + i)m - r, \quad r''' = m + ir'' = im - ir$$

hat, und man annimmt, dass die erste r zum Complexe C gehört, so werden die übrigen r', r'', r''' respective zu den Complexen C', C'', C''' gehören.

Denn setzt man:

$$\begin{aligned} \xi &= ax + by, & \eta &= ay - bx \\ \xi' &= ax' + by', & \eta' &= ay' - bx' \\ \xi'' &= ax'' + by'', & \eta'' &= ay'' - bx'' \\ \xi''' &= ax''' + by''', & \eta''' &= ay''' - bx''', \end{aligned}$$

so findet man:

$$\eta = p - \xi' = p - \eta'' = \xi'''$$
$$\xi - \eta = \xi' + \eta' - p = \eta'' - \xi'' = p - \xi''' - \eta'''$$
$$p - \xi - \eta = \xi' - \eta' = \xi'' + \eta'' - p = \eta''' - \xi''',$$

woraus sich mit Hülfe der Kriterien für die einzelnen Complexe die Richtigkeit des Satzes von selbst ergiebt. Und da wiederum $r = m + ir'''$ ist, so sieht man leicht, dass, wenn r zum Complex C' gehörig vorausgesetzt wird, die Zahlen r', r'', r''' respective zu C'', C''', C gehören; gehört jene zu C'', so gehören diese zu C''', C, C'; gehört endlich jene zu C''', so gehören diese zu C, C', C''.

Gleichzeitig folgt hieraus, dass in den einzelnen Complexen C, C', C'', C''' gleichviel Zahlen enthalten sind, nämlich $\frac{1}{4}(p-1)$.

71.

Satz. Werden, unter k eine ganze durch m nicht teilbare Zahl verstanden, die einzelnen Zahlen des Complexes C mit k multipliciert und wird, nachdem die einfach kleinsten Reste dieser Producte nach dem Modul m unter die Complexe C, C', C'', C''' verteilt sind, die Anzahl derjenigen, welche zu diesen einzelnen Complexen gehören, respective mit c, c', c'', c''', bezeichnet, so ist der Character der Zahl k in Bezug auf den Modul m congruent $c' + 2c'' + 3c'''$ (mod. 4).

Beweis. Es seien die c zu C gehörigen kleinsten Reste $\alpha, \beta, \gamma, \delta, \ldots$, die c' zu C' gehörigen Reste $m + i\alpha'$, $m + i\beta'$, $m + i\gamma'$, $m + i\delta'$, ..., ferner die c'' zu C'' gehörigen Reste $(1+i)m - \alpha''$, $(1+i)m - \beta''$, $(1+i)m - \gamma''$, $(1+i)m - \delta''$, ..., endlich die c''' zu C''' gehörigen Reste $im - i\alpha'''$, $im - i\beta'''$, $im - i\gamma'''$, $im - i\delta'''$, ... Wir betrachten nun vier Producte, nämlich:

1. das Product aus allen $\frac{1}{4}(p-1)$ den Complex C bildenden Zahlen,
2. das Product der Producte, welche aus der Multiplikation dieser einzelnen Zahlen mit k entstehen,
3. das Product aus den kleinsten Resten dieser Producte, nämlich aus den Zahlen $\alpha, \beta, \gamma, \delta, \ldots, m + i\alpha', m + i\beta', \ldots$.
4. das Product aus allen $c + c' + c'' + c'''$ Zahlen $\alpha, \beta, \gamma, \delta, \ldots, \alpha', \beta', \gamma', \delta', \ldots, \alpha'', \beta'', \gamma'', \delta'', \ldots$.

Bezeichnet man diese vier Producte der Reihe nach mit P, P', P'', P''', so ist offenbar:

$$P' = k^{\frac{1}{4}(p-1)}P, \quad P' \equiv P'', \quad P'' \equiv P'''i^{c'+2c''+3c'''} \pmod{m}$$

und somit:

$$Pk^{\frac{1}{4}(p-1)} \equiv P'''i^{c'+2c''+3c'''} \pmod{m}.$$

Man sieht aber leicht, dass die Zahlen $\alpha', \beta', \gamma', \delta', \ldots, \alpha'', \beta'', \gamma'', \delta'', \ldots,$ $\alpha''', \beta''', \gamma''', \delta''', \ldots$ sämtlich zum Complexe C gehören und sowohl unter sich als auch von den Zahlen $\alpha, \beta, \gamma, \delta, \ldots$ verschieden sind, ebenso wie diese selbst unter einander verschieden sind. Daher müssen alle diese Zahlen zusammengenommen und abgesehen von der Reihenfolge vollständig identisch sein mit allen den Complex C bildenden Zahlen, woraus folgt $P = P'''$ und daher:

$$Pk^{\frac{1}{4}(p-1)} \equiv Pi^{c'+2c''+3c'''} \pmod{m}.$$

Schliesslich ergiebt sich hieraus, da die einzelnen Factoren des Products P durch m nicht teilbar sind,

$$k^{\frac{1}{4}(p-1)} \equiv i^{c'+2c''+3c'''} \pmod{m},$$

so dass $c' + 2c'' + 3c'''$ der Character der Zahl k in Bezug auf den Modul m ist.

72.

Um das allgemeine Theorem des vorigen Artikels auf die Zahl $1 + i$ anwenden zu können, müssen wir den Complex C wiederum in zwei kleinere Complexe G und G' teilen und zwar werden wir zum Complex G diejenigen Zahlen $x + yi$ rechnen, für welche $ax + by = \xi$ kleiner ist als $\frac{1}{2}p$, zum Complexe G' aber diejenigen, für welche ξ grösser als $\frac{1}{2}p$ ist; die Anzahl der in den Complexen G und G' enthaltenen Zahlen werden wir mit g und g' bezeichnen, so dass $g + g' = \frac{1}{4}(p-1)$ ist.

Das vollständige Kriterium der zum Complexe G gehörigen Zahlen ist somit, dass die drei Zahlen η, $\xi - \eta$, $p - 2\xi$ positiv sind; denn die dritte Bedingung für den Complex C, nach welcher $p - \xi - \eta$ positiv sein soll, ist bereits implicite unter jenen enthalten, da $p - \xi - \eta = (\xi - \eta) + (p - 2\xi)$ ist. Ebenso besteht das vollständige Kriterium der zu G' gehörigen Zahlen in positiven Werten der drei Zahlen η, $p - \xi - \eta$, $2\xi - p$.

Hieraus folgt leicht, dass das Product einer jeden Zahl des Complexes G mit der Zahl $1 + i$ zum Complex C''' gehört. Denn setzt man:

$$(x + yi)(1 + i) = x' + y'i \text{ und } ax' + by' = \xi', \; ay' - bx' = \eta',$$

so findet man:

$$\xi' = \xi - \eta, \quad \eta' - \xi' = 2\eta, \quad p - \xi' - \eta' = p - 2\xi,$$

d. h. das Kriterium für die dem Complex G zugehörige Zahl $x + yi$ ist identisch mit dem Kriterium für die zum Complex C''' gehörige Zahl $x' + y'i$.

Auf ganz ähnliche Weise zeigt man, dass das Product einer jeden Zahl des Complexes G' mit $1+i$ zum Complex C'' gehört.

Es ist daher, wenn wir im vorigen Artikel k den Wert $1+i$ beilegen, $c=0$, $c'=0$, $c''=g'$, $c'''=g$, und somit wird der Character der Zahl $1+i$: $3g+2g'=\frac{1}{2}(p-1)+g$. Und da die Charactere der Zahlen i, -1 respective $\frac{1}{4}(p-1)$, $\frac{1}{2}(p-1)$ sind, so werden die Charactere der Zahlen $-1+i$, $-1-i$, $1-i$ respective $\frac{3}{4}(p-1)+g$, g, $\frac{1}{4}(p-1)+g$ sein. Somit handelt es sich nur noch um die Ermittlung der Zahl g.

73.

Die Auseinandersetzungen in den Artikeln 69 bis 72 sind eigentlich unabhängig von der Voraussetzung, dass m eine primäre Zahl sei; von nun an wollen wir aber wenigstens annehmen, dass a ungerade, b gerade sei, und ausserdem dass a, b und $a-b$ positive Zahlen seien. Vor allen Dingen müssen wir die Grenzen der Werte von x in dem Complexe G feststellen.

Setzt man:

$$ay-bx=\eta, \quad (a+b)x-(a-b)y=\zeta, \quad p-2ax-2by=\vartheta,$$

so besteht das Kriterium der zum Complexe G gehörigen Zahlen $x+yi$ in den drei Bedingungen, dass η, ζ, ϑ positive Zahlen seien. Da $px=(a-b)\eta+a\zeta$, $p(a-2x)=a\vartheta+2b\eta$ wird, so müssen offenbar x und $2a-x$ positive Zahlen, oder es muss x irgend einer der Zahlen $1, 2, 3, \ldots, \frac{1}{2}(a-1)$ gleich sein. Da ferner $(a-b)\vartheta=2b\zeta+p(a-b-2x)$ ist, so ist klar, dass, sobald x kleiner als $\frac{1}{2}(a-b)$ ist, die zweite Bedingung (nach welcher ζ positiv sein soll) bereits die dritte (dass ϑ positiv sein muss) in sich schliesst, dass dagegen, sooft x grösser als $\frac{1}{2}(a-b)$ ist, die zweite Bedingung bereits unter der dritten enthalten ist. Mithin hat man nur für die folgenden Werte von x, nämlich $1, 2, 3, \ldots, \frac{1}{2}(a-b-1)$, dafür zu sorgen, dass η und ζ positiv werden, oder dass y grösser als $\frac{bx}{a}$ und kleiner als $\frac{(a+b)x}{a-b}$ sei. Für einen gegebenen derartigen Wert von x giebt es daher Zahlen $x+yi$ im Ganzen

$$\left[\frac{(a+b)x}{a-b}\right]-\left[\frac{bx}{a}\right],$$

wenn wir uns der eckigen Klammern in derselben Bedeutung bedienen, in welcher wir sie anderswo vorübergehend gebraucht haben [Vgl. „*Neuer Beweis eines arithm. Satzes*“, Art. 4 (oben S. 459) und „*Neue Beweise und Erweit. des Fundamentalsatzes i. d. Lehre v. d. quadr. Resten*“, *Neuer Algorithmus u. s. w.* Artikel 3 (oben S. 507)]. Dagegen genügt es für die folgenden Werte von x: $\frac{1}{2}(a-b+1)$, $\frac{1}{2}(a-b+3)$, $\ldots$, $\frac{1}{2}(a-1)$, wenn

η und ϑ positive Werte erhalten, oder wenn y grösser als $\frac{bx}{a}$ und kleiner als $\frac{p-2ax}{2b}$ oder $\frac{1}{2}b+\frac{a^2-2ax}{2b}$ wird; mithin giebt es für einen gegebenen derartigen Wert von x Zahlen $x+yi$ im Ganzen:

$$\left[\tfrac{1}{2}b+\frac{a^2-2ax}{2b}\right]-\left[\frac{bx}{a}\right].$$

Hieraus schliessen wir daher, dass die Anzahl der Zahlen des Complexes G ist:

$$g=\sum\left[\frac{(a+b)x}{a-b}\right]+\sum\left[\tfrac{1}{2}b+\frac{a^2-2ax}{2b}\right]-\sum\left[\frac{bx}{a}\right],$$

wo im ersten Gliede die Summation über alle ganzen Werte von x von 1 bis $\frac{1}{2}(a-b-1)$, im zweiten von $\frac{1}{2}(a-b+1)$ bis $\frac{1}{2}(a-1)$, im dritten von 1 bis $\frac{1}{2}(a-1)$ auszudehnen ist.

Wenn wir uns des Buchstabens φ in derselben Bedeutung bedienen, wie am angeführten Orte (vgl. oben S. 507), nämlich, dass

$$\varphi(t, u)=\left[\frac{u}{t}\right]+\left[\frac{2u}{t}\right]+\left[\frac{3u}{t}\right]+\cdots+\left[\frac{t'u}{t}\right]$$

sein solle, wo t, u irgend welche positive Zahlen bezeichnen und t' die Zahl $[\frac{1}{2}t]$ bedeutet, so ist jenes erste Glied gleich $\varphi(a-b, a+b)$, das dritte gleich $-\varphi(a, b)$, das zweite aber wird gleich

$$\tfrac{1}{4}b^2+\sum\left[\frac{a^2-2ax}{2b}\right].$$

Es ist aber, wenn wir die Glieder in umgekehrter Reihenfolge schreiben:

$$\sum\left[\frac{a^2-2ax}{2b}\right]=\left[\frac{a}{2b}\right]+\left[\frac{3a}{2b}\right]+\left[\frac{5a}{2b}\right]+\cdots+\left[\frac{(b-1)a}{2b}\right]$$
$$=\varphi(2b, a)-\varphi(b, a).$$

Daher nimmt unsere Formel die folgende Form an:

$$g=\varphi(a-b, a+b)+\varphi(2b, a)-\varphi(a, b)-\varphi(b, a)+\tfrac{1}{4}b^2.$$

Wir betrachten zuerst das Glied $\varphi(a-b, a+b)$, welches sich sogleich verwandelt in $\varphi(a-b, 2b)+1+2+3+\cdots+\frac{1}{2}(a-b-1)$ oder in

$$\varphi(a-b, 2b)+\tfrac{1}{8}\big((a-b)^2-1\big).$$

Ferner haben wir, da nach dem allgemeinen Satze $\varphi(t, u)+\varphi(u, t) = [\frac{1}{2}t]\cdot[\frac{1}{2}u]$ wird, sobald t und u zu einander prime positive ganze Zahlen sind:

$$\varphi(a-b, 2b)=\tfrac{1}{2}b(a-b-1)-\varphi(2b, a-b)$$

und daher:

$$\varphi(a-b,\ a+b)=\tfrac{1}{8}(a^2+2ab-3b^2-4b-1)-\varphi(2b,\ a-b).$$

Ordnen wir die Glieder von $\varphi(2b,\ a-b)$ in folgender Weise an:

$$\left[\frac{a-b}{2b}\right]+\left[\frac{3(a-b)}{2b}\right]+\left[\frac{5(a-b)}{2b}\right]+\cdots+\left[\frac{(b-1)(a-b)}{2b}\right]$$
$$+\left[\frac{a-b}{b}\right]+\left[\frac{2(a-b)}{b}\right]+\left[\frac{3(a-b)}{b}\right]+\cdots+\left[\frac{\frac{1}{2}b(a-b)}{b}\right],$$

so wird die zweite Reihe offenbar gleich

$$\varphi(b,\ a-b)=\varphi(b,\ a)-1-2-3-\cdots-\tfrac{1}{2}b=\varphi(b,\ a)-\tfrac{1}{8}(b^2+2b);$$

die erste Reihe aber stellen wir nach Umkehrung der Reihenfolge der Glieder so dar:

$$\left[\tfrac{1}{2}(a+1-b)-\frac{a}{2b}\right]+\left[\tfrac{1}{2}(a+3-b)-\frac{3a}{2b}\right]+\left[\tfrac{1}{2}(a+5-b)-\frac{5a}{2b}\right]+\cdots$$
$$+\left[\tfrac{1}{2}(a-1)-\frac{(b-1)a}{2b}\right],$$

und dieser Ausdruck verwandelt sich, da, wenn t eine ganze, u eine gebrochene Zahl bezeichnet, allgemein $[t-u]=t-1-[u]$ ist, in folgenden:

$$\tfrac{1}{8}b(2a-4-b)-\left[\frac{a}{2b}\right]-\left[\frac{3a}{2b}\right]-\left[\frac{5a}{2b}\right]-\cdots-\left[\frac{(b-1)a}{2b}\right]$$
$$=\tfrac{1}{8}b(2a-4-b)-\varphi(2b,\ a)+\varphi(b,\ a).$$

Hiernach wird:

$$\varphi(2b,\ a-b)=2\varphi(b,\ a)-\varphi(2b,\ a)+\tfrac{1}{4}b(a-3-b)$$

und somit:

$$\varphi(a-b,\ a+b)=\varphi(2b,\ a)-2\varphi(b,\ a)+\tfrac{1}{8}(a^2-b^2+2b-1).$$

Substituiert man diesen Wert in die oben für g angegebene Formel und setzt überdies $\varphi(a,\ b)+\varphi(b,\ a)=\tfrac{1}{4}b(a-1)$, so erhält man:

$$g=2\varphi(2b,\ a)-2\varphi(b,\ a)+\tfrac{1}{8}(a^2-2ab+b^2+4b-1).$$

74.

Durch ganz ähnliche Schlüsse erledigt sich der Fall, wo zwar a, b positiv bleiben, aber $a-b$ negativ oder $b-a$ positiv ist. Die Gleichungen $p(a-2x)=2b\eta+a\vartheta$, $p(b-a+2x)=2b\zeta+(b-a)\vartheta$ zeigen, dass $\tfrac{1}{2}a-x$ und $x+\tfrac{1}{2}(b-a)$ positiv und somit x irgend einer der Zahlen $-\tfrac{1}{2}(b-a-1)$, $-\tfrac{1}{2}(b-a-3)$, $-\tfrac{1}{2}(b-a-5)$, ..., $+\tfrac{1}{2}(a-1)$ gleich sein muss. Ferner folgt aus der Gleichung $px+(b-a)\eta=a\zeta$, dass für negative Werte von x die Bedingung, nach welcher η positiv sein soll, bereits unter

der Bedingung, nach welcher ζ positiv sein soll, enthalten ist, dass aber das Gegenteil stattfindet, sobald x ein positiver Wert beigelegt wird. Hiernach müssen die Werte von y für einen bestimmten negativen Wert von x zwischen $\frac{(a+b)x}{a-b}$ und $\frac{p-2ax}{2b}$, für einen gegebenen positiven Wert von x aber zwischen $\frac{bx}{a}$ und $\frac{p-2ax}{2b}$ enthalten sein; offenbar sind für $x=0$ diese Grenzen 0 und $\frac{p}{2b}$, mit Ausschluss des Wertes $y=0$ selbst. Hieraus folgt:

$$g=-\sum\left[\frac{(a+b)x}{a-b}\right]+\sum\left[\tfrac{1}{2}b+\frac{a^2-2ax}{2b}\right]-\sum\left[\frac{bx}{a}\right],$$

wo in dem ersten Gliede die Summation über alle negativen Werte von x von -1 an bis $-\frac{1}{2}(b-a-1)$, im zweiten über alle Werte von x von $-\frac{1}{2}(b-a-1)$ an bis $\frac{1}{2}(a-1)$, im dritten über alle positiven Werte von x von $+1$ an bis zu $\frac{1}{2}(a-1)$ zu erstrecken ist. Auf diese Weise ergiebt sich aus der ersten Summation $-\varphi(b-a,\ b+a)$, aus der zweiten ebenso wie im vorigen Artikel $\frac{1}{4}b^2+\varphi(2b,\ a)-\varphi(b,\ a)$, endlich aus der dritten $-\varphi(a,\ b)$, oder man hat:

$$g=-\varphi(b-a,\ b+a)+\varphi(2b,\ a)-\varphi(b,\ a)-\varphi(a,\ b)+\tfrac{1}{4}b^2.$$

Auf ganz ähnliche Weise wie im vorigen Artikel entwickelt man nun:

$$\begin{aligned}\varphi(b-a,b+a)&=\varphi(b-a,\ 2b)-\tfrac{1}{8}\big((b-a)^2-1\big)\\&=\tfrac{1}{8}(3b^2-2ab-a^2-4b+1)-\varphi(2b,\ b-a),\end{aligned}$$

sowie:

$$\varphi(2b,\ b-a)=\varphi(2b,a)-2\varphi(b,a)+\tfrac{1}{4}b(b-1-a)$$

und daher:

$$\varphi(b-a,b+a)=2\varphi(b,a)-\varphi(2b,a)+\tfrac{1}{8}(b^2-a^2-2b+1)$$

und schliesslich:

$$g=2\varphi(2b,a)-2\varphi(b,a)+\tfrac{1}{8}(a^2-2ab+b^2+4b-1).$$

Es ist daher bewiesen, dass für g dieselbe Formel gilt, mag $a-b$ positiv oder negativ sein, wofern nur a, b positiv sind.

75.

Um eine weitere Reduction zu erlangen, setzen wir:

$$\begin{aligned}L&=\left[\frac{a}{2b}\right]+\left[\frac{2a}{2b}\right]+\left[\frac{3a}{2b}\right]+\cdots+\left[\frac{\frac{1}{2}ba}{2b}\right]\\M&=\left[\frac{(\frac{1}{2}b+1)a}{2b}\right]+\left[\frac{(\frac{1}{2}b+2)a}{2b}\right]+\left[\frac{(\frac{1}{2}b+3)a}{2b}\right]+\cdots+\left[\frac{ba}{2b}\right]\\N&=\left[\frac{a+b}{2b}\right]+\left[\frac{2a+b}{2b}\right]+\left[\frac{3a+b}{2b}\right]+\cdots+\left[\frac{\frac{1}{2}ba+b}{2b}\right].\end{aligned}$$

Da man leicht sieht, dass allgemein $[u]+[u+\frac{1}{2}]=[2u]$ ist, welche reelle Grösse auch immer u bezeichnen möge, so wird $L+N=\varphi(b,a)$, und da offenbar $L+M=\varphi(2b,a)$ ist, so wird:

$$\varphi(2b,a)-\varphi(b,a)=M-N.$$

Ferner ist klar, dass das Aggregat des ersten Gliedes der Reihe N und des vorletzten Gliedes der Reihe M, nämlich $\left[\frac{a+b}{2b}\right]+\left[\frac{(b-1)a}{2b}\right]=\frac{1}{2}(a-1)$ wird, und dass dieselbe Summe von dem zweiten Gliede der Reihe N und dem vorvorletzten der Reihe M gebildet wird u. s. w. Da nun auch das letzte Glied der Reihe M gleich $\frac{1}{2}(a-1)$ ist, das letzte Glied der Reihe N aber gleich $\left[\frac{a+2}{4}\right]=\frac{1}{4}(a\mp 1)$ ist, wo das obere oder untere Vorzeichen gilt, je nachdem a von der Form $4n+1$ oder $4n-1$ ist, so folgt:

$$M+N=\tfrac{1}{4}(a-1)b+\tfrac{1}{4}(a\mp 1),$$

und somit:

$$\varphi(2b,a)-\varphi(b,a)=\tfrac{1}{4}(a-1)b+\tfrac{1}{4}(a\mp 1)-2N.$$

Demnach geht die für g in den Artikeln 73 und 74 gefundene Formel in die folgende über:

$$g=\tfrac{1}{8}\big((a+b)^2-1\big)+2n-4N,$$

wenn man $a\mp 1=4n$ setzt, wo n eine ganze Zahl ist. Da man aber hieraus $1=16n^2-8an+a^2$ erhält, so kann diese Formel auch folgendermassen dargestellt werden:

$$g=\tfrac{1}{8}(-a^2+2ab+b^2+1)+4\big(\tfrac{1}{2}(a+1)n-n^2-N\big).$$

Da nun g der Character der Zahl $-1-i$ für den Modul $a+bi$ ist, so wird demnach dieser Character $\equiv\frac{1}{8}(-a^2+2ab+b^2+1)$ (mod. 4), und dieses ist gerade der oben (Artikel 64) durch Induction gefundene Satz, und hieraus ergeben sich unmittelbar die Sätze bezüglich der Charactere der Zahlen $1+i$, $1-i$, $-1+i$. Mithin sind diese vier Sätze für denjenigen Fall, in welchem a, b positiv sind, nunmehr in aller Strenge bewiesen.

76.

Ist b negativ, während a positiv bleibt, so setze man $b=-b'$, so dass b' positiv wird. Da nun bewiesen worden ist, dass für den Modul $a+b'i$ der Character der Zahl $-1-i$ congruent $\frac{1}{8}(-a^2+2ab'+b'^2+1)$ (mod. 4) ist, so wird der Character der Zahl $-1+i$ für den Modul $a-b'i$ nach dem im Artikel 62 angeführten Satze $\equiv\frac{1}{8}(a^2-2ab'-b'^2-1)$ sein, d. h. der Character der Zahl $-1+i$ für den Modul $a+bi$ ist $\equiv\frac{1}{8}(a^2+2ab-b^2-1)$; dies aber ist gerade der im Artikel 64 angegebene Satz, woraus sich die drei übrigen auf die Charactere der Zahlen $1+i$,

$1-i$, $-1-i$ bezüglichen von selbst ergeben. Mithin sind diese Sätze auch für den Fall, wo b negativ ist, bewiesen, d. h. für alle Fälle, in denen a positiv ist.

Ist endlich a negativ, so setze man $a=-a'$, $b=-b'$. Da nun nach dem bereits Bewiesenen der Character der Zahl $1+i$ hinsichtlich des Moduls $a'+b'i$ ist: $\equiv \frac{1}{8}(-a'^2+2a'b'-3b'^2+1) \pmod{4}$ und es gleichgültig ist, ob wir die Zahl $a'+b'i$ oder die entgegengesetzte $-a'-b'i$ als Modul haben, so ist der Character der Zahl $1+i$ in Bezug auf den Modul $a+bi$ offenbar $\equiv \frac{1}{8}(-a^2+2ab-3b^2+1) \pmod{4}$, und Ähnliches gilt von den Characteren der Zahlen $1-i$, $-1+i$, $-1-i$.

Hieraus folgt daher, dass der Beweis der Sätze über die Charactere der Zahlen $1+i$, $1-i$, $-1+i$, $-1-i$ (Artikel 63 und 64) keiner Beschränkung mehr unterliegt.

Einige Untersuchungen

aus dem

handschriftlichen Nachlasse von Gauss.



Die Lehre von den Resten.

I.

Lösung der Congruenz $X^m - 1 \equiv 0$.

237.*)

Im dritten Kapitel haben wir gezeigt, dass die Congruenz $x^n \equiv 1$, wenn eine Primzahl p zum Modul genommen wird, μ Wurzeln besitzt, falls μ der grösste gemeinschaftliche Teiler der Zahlen n und $p-1$ ist, und dass diese Wurzeln mit den Wurzeln der Congruenz $x^\mu \equiv 1$ völlig übereinstimmen. Daher genügt es, denjenigen Fall zu betrachten, wo n ein aliquoter Teil von $p-1$ ist. Dass man aber die Lösung nicht nur dieser Congruenz $x^n \equiv 1$, sondern auch jeder andern für beliebige Moduln aus der Lösung für Moduln, welche Primzahlen sind, ableiten könne, ist bereits vorübergehend gezeigt worden und wird unten (im achten Kapitel) weitläufiger gelehrt werden.

238.

Aber auch hier braucht man noch nicht stehen zu bleiben; denn in demselben Kapitel haben wir dargelegt, dass die Lösung der Congruenz $x^n \equiv 1$ von der Auflösung ähnlicher Congruenzen $x^a \equiv 1$, $x^b \equiv 1, \ldots$ abhängt, wo a, b, ... Primzahlen oder Potenzen von Primzahlen sind und n das Product aus diesen Zahlen ist. Sind nämlich A, B, ... respective irgend welche Wurzeln der Congruenzen $x^a \equiv 1$, $x^b \equiv 1$, ..., so ist das Product aus diesen $AB \ldots$ eine der Wurzeln der Congruenz $x^n \equiv 1$. Wir werden daher unsere Untersuchungen auf die Lösung der Congruenz $x^n \equiv 1$ (mod. p) beschränken, wo p eine Primzahl, n eine Primzahl oder die Potenz einer Primzahl und zugleich ein aliquoter Teil der Zahl $p-1$ ist.

*) Vgl. das Vorwort des Herausgebers.

239.

Ferner ist aus dem dritten Kapitel bekannt, dass es unter den Wurzeln der Congruenz $x^n \equiv 1$ stets solche giebt, durch deren Potenzen alle übrigen dargestellt werden können. So werden, wenn r eine derartige Wurzel bezeichnet (wir nannten sie oben eine primitive Wurzel, wenn $n = p - 1$ war, und diesen Ausdruck wollen wir hier obwohl in weiterer Bedeutung beibehalten), sämtliche Wurzeln der gegebenen Congruenz sein:

$$1,\ r,\ r^2,\ r^3,\ \ldots,\ r^{n-1}.$$

Wir werden also alle unsere Bemühungen darauf richten müssen, derartige Wurzeln zu ermitteln, da, wenn diese gefunden sind, die übrigen von selbst sich ergeben. Der Kürze halber bezeichnen wir irgend eine Potenz von r durch ihren in Klammern eingeschlossenen Exponenten, so dass (0) die Einheit, (1) irgend eine primitive Wurzel der Congruenz $x^n \equiv 1$, (2) das Quadrat von (1) u. s. w. bedeutet und daher die Reihe (0), (1), (2), (3), . . ., $(n-1)$ alle Wurzeln umfasst. Uebrigens ist bekanntlich (k) immer eine solche primitive Wurzel, sooft k zu n prim ist, d. h. in unserem Falle (wo n eine Potenz der Primzahl t etwa gleich t^ν ist), sooft t in k nicht aufgeht. Offenbar aber sind die Bezeichnungen (1), (2), . . . an sich unbestimmt, sobald aber (1) irgend ein bestimmter Wert beigelegt wird, werden auch alle übrigen bestimmt werden.

240.

Da wir uns vorgenommen haben, vor allem die primitiven Wurzeln zu suchen, so müssen wir diese zunächst von den übrigen separieren. Dies geschieht, wenn wir aus der Reihe (0), (1), (2), . . ., $(n-1)$ alle Glieder weglassen, in denen k durch t teilbar ist; wenn aber n eine Primzahl oder $\nu = 0$ ist, so wird nur das eine (0) wegzulassen sein. Bevor wir aber zur Untersuchung der übrigen fortschreiten, empfehlen wir dem Leser sehr, sich einige Beispiele zu bilden, damit er alles, was ohne diese vielleicht als zu allgemein gehalten erscheinen möchte, in concreto vor sich habe. Wir fügen zwar hier ein **Beispiel** hinzu, doch wird es darum nicht überflüssig sein, andere auf eigene Hand zu berechnen.

Ist $p = 29$, $n = 7$, so sind die sieben Wurzeln der Congruenz $x^7 \equiv 1$ (mod. 29): 1, 7, 16, 20, 23, 24, 25. Da n eine Primzahl ist, so werden alle diese Wurzeln ausser 1 primitive Wurzeln sein; setzt man also $7 = (1)$, so werden die Zeichen

(0), (1), (2), (3), (4), (5), (6)

respective folgende Bedeutung haben:

1, 7, 20, 24, 23, 16, 25.

Übrigens wird man sich erinnern, dass die Zeichen (n) und (0), $(n+1)$ und (1), u. s. w. und allgemein (a) und (b) äquivalent sind, wenn $a \equiv b$ (mod. n) ist.

241.

Um aber unsern Zweck zu erreichen, müssen wir noch in anderer Weise verfahren. Wir behalten nämlich nur diejenigen Glieder (k) bei, in den k durch t nicht teilbar ist und deren Anzahl gleich $\frac{t-1}{t} \cdot n = \lambda$ ist; alle diese Zahlen aber (oder die ihnen nach dem Modul n congruenten) lassen sich durch die aufeinanderfolgenden Potenzen irgend einer Zahl darstellen.

Ist diese gleich ρ, so werden alle primitiven Wurzeln der Congruenz $x^n \equiv 1$ folgendermassen bezeichnet werden:

$$(1), (\rho), (\rho^2), (\rho^3), \ldots\ldots, (\rho^{\lambda-1}).$$

Durch diesen Kunstgriff aber erreichen wir, dass sämtliche nicht primitiven Wurzeln vollständig ausgeschlossen werden; die Gründe und Vorteile hiervon wird man unten deutlicher erkennen. In unserm Beispiel können wir also $\rho = 3$ setzen; dann werden sich die primitiven Wurzeln der Congruenz $x^7 \equiv 1$ so anordnen:

	(1),	(3),	(3^2),	(3^3),	(3^4),	(3^5)
oder:	(1),	(3),	(2),	(6),	(4),	(5)
und diese sind:	7,	24,	20,	25,	23,	16.

242.

Damit der Leser wisse, wohin die folgenden Untersuchungen abzielen, wollen wir den **Satz** angeben, dessen Beweis und Erläuterung wir uns vorgenommen haben.

Wenn die Zahl λ (welche gleich $t^{\nu-1} \cdot t - 1$ ist) die einfachen Factoren $a, b, c, d, \ldots$ hat und $\lambda = a^\alpha b^\beta c^\gamma \ldots$ ist, so hängt die Lösung der Congruenz $x^n - 1 \equiv 0$ von der Lösung von $\alpha + \beta + \cdots$ niedrigeren Congruenzen ab, von denen α vom Grade a, β vom Grade b, γ vom Grade c, u. s. w. sind.

So hängt in unserm Beispiel die Lösung der Congruenz $x^7 \equiv 1$ von einer Congruenz zweiten Grades und von einer andern dritten Grades ab, und man sieht allgemein, dass niemals der Grad dieser Congruenzen von dem Modul p abhängt. Um aber zum Beweise dieses Satzes zu gelangen, müssen wir einige den Zusammenhang der Congruenzen und ihrer Wurzeln betreffende Sätze vorausschicken, obwohl diese Untersuchungen eigentlich erst im achten Kapitel weiter zu verfolgen sind.

243.

Satz. Wenn die Congruenz

$$x^m + Ax^{m-1} + Bx^{m-2} + \cdots + N \equiv 0 \text{ (nach einem Primzahlmodul)}$$

so beschaffen ist, dass nach Ausführung des Productes aus den m Factoren $x - r$, $x - r'$, $x - r''$, $x - r'''$, ..., wodurch dasselbe

$x^m + ax^{m-1} + bx^{m-2} + \cdots + n$ werden möge, $A \equiv a$, $B \equiv b$, $C \equiv c, \ldots$ nach dem Modul p ist, so werden die Grössen $r, r', r'', \ldots$ Wurzeln der gegebenen Congruenz sein, und zwar wird dieselbe keine andern Wurzeln haben.

Beweis. I. Es ist stets

$$x^m + Ax^{m-1} + Bx^{m-2} + \cdots \equiv x^m + ax^{m-1} + bx^{m-2} + \cdots \pmod{p}.$$

Die rechte Seite der Congruenz wird aber $= 0$, wenn man $x = r$, $x = r'$, $x = r'', \ldots$ setzt; daher wird für diese Werte von x die linke Seite $\equiv 0 \pmod{p}$. Dies ist der erste Teil des Satzes.

II. Wenn aber noch ein anderer Wert ρ, welcher keiner der Zahlen $r, r', r'', \ldots$ congruent ist, der gegebenen Congruenz genügte, so würde sein:

$$\begin{aligned} 0 &\equiv \rho^m + A\rho^{m-1} + B\rho^{m-2} + \cdots \equiv \rho^m + a\rho^{m-1} + b\rho^{m-2} + \cdots \\ &\equiv (\rho - r)(\rho - r')(\rho - r'')(\rho - r''') \ldots . \end{aligned}$$

Da aber keiner der Factoren $\rho - r$, $\rho - r'$, $\rho - r'', \cdots \equiv 0$ ist, so müsste das Product aus allen der Null congruent werden, was absurd ist. Daher giebt es ausser den Wurzeln $r, r', \ldots$ keine andern Wurzeln. Dies ist der zweite Teil des Satzes.

244.

Aufgabe. Es seien $r, r', r'', \ldots$ unbekannte Grössen, deren Anzahl gleich m sei, und es sei die Summe derselben gleich α, die Summe ihrer Quadrate gleich β, die Summe der Kuben gleich γ u. s. w., die Summe ihrer m^{ten} Potenzen gleich μ; es sollen aber nicht diese Zahlen selbst (deren Anzahl ebenfalls gleich m ist) gegeben sein, sondern andere, $\alpha', \beta', \gamma', \ldots$, welche ihnen einzeln nach dem Modul p, der eine Primzahl und grösser als m sei, congruent sind. Dann soll man die Congruenz m^{ten} Grades finden, deren Wurzeln $r, r', r'', \ldots$ sind.

Auflösung. Man betrachte $r, r', r'', \ldots$ als Wurzeln einer Gleichung

$$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} + \cdots = 0$$

und bestimme ihre Coefficienten $A, B, C, \ldots$ (indem man nur die Congruenz an Stelle der Gleichung anwendet) nach der bekannten Methode, indem man nämlich setzt:

$$\begin{aligned} -A &\equiv \alpha' \\ -2B &\equiv \beta' + A\alpha' \\ -3C &\equiv \gamma' + A\beta' + B\alpha' \\ -4D &\equiv \delta' + A\gamma' + B\beta' + C\alpha' \\ &\ldots\ldots\ldots\ldots \\ -mN &\equiv \mu' + A\lambda' + \cdots \end{aligned}$$

Diese Coefficienten können aber nicht unbestimmt sein, weil alle Zahlen $1, 2, 3, \ldots, n < p$ sind. Dann behaupte ich, dass die Congruenz

$$x^m + Ax^{m-1} + Bx^{m-2} + \cdots + N \equiv 0$$

die gesuchte ist.

Beweis. Nimmt man an, dass die Gleichung, deren Wurzeln r, r', r'', r''', ... sind, die folgende sei:

$$x^m + ax^{m-1} + bx^{m-2} + \cdots = 0,$$

so wird:

$$\begin{aligned} -\ a &= \alpha \\ -2b &= \beta + a\alpha \\ -3c &= \gamma + a\beta + b\alpha \\ -4d &= \delta + a\gamma + b\beta + c\alpha \\ &\ldots\ldots\ldots \end{aligned}$$

Offenbar aber wird hiernach

$$a \equiv A,\quad b \equiv B,\quad c \equiv C, \ldots \pmod{p},$$

und daher werden nach dem vorhergehenden Artikel die Zahlen $r, r', r'', \ldots$, welche Wurzeln der Gleichung

$$x^m + ax^{m-1} + bx^{m-2} + \cdots = 0$$

sind, zugleich Wurzeln der Congruenz

$$x^m + Ax^{m-1} + Bx^{m-2} + \cdots \equiv 0$$

sein.

Wir überlassen es dem Leser, sich Beispiele zu bilden.

245.

Wir kehren zu unsrer Aufgabe zurück. Unter Beibehaltung der in dem Artikel 242 und den vorhergehenden Artikeln angewandten Bezeichnungen, wollen wir zeigen, dass, wenn λ das Product aus irgend welchen Factoren $efg \ldots$ ist, die primitiven Wurzeln der Congruenz $x^n \equiv 1$, deren Anzahl gleich λ ist, so in e Klassen geteilt werden können, dass die Aggregate der zu derselben Klasse gerechneten Wurzeln durch eine Congruenz vom e^{ten} Grade gegeben werden, dass ferner, wenn man diese als bekannt voraussetzt, jede Klasse weiter so in f Ordnungen geteilt werden kann, dass die Aggregate jeder Ordnung durch eine Congruenz f^{ten} Grades gegeben werden, und diese Ordnungen lassen sich wiederum teilen u. s. w., bis man zu den einzelnen Wurzeln gelangt.

246.

Definition. Den Complex aller in einer solchen Form $(\rho^{ke+\alpha})$ (Artikel 241) enthaltenen Glieder werden wir eine **vollständige Periode** oder

einfach eine Periode nennen. Es bezeichnet aber e irgend einen Teiler der Zahl λ, α irgend eine gegebene Zahl, k alle ganzen Zahlen von 0 bis $\frac{\lambda}{e}-1$, und der Kürze wegen werden wir eine solche Periode mit $(e*\alpha)$ bezeichnen. So bilden in unserm Beispiele die Glieder

	(1), (2), (4)	die Periode	$(2*0)$
	(3), (6), (5)	„	$(2*1)$
aber	(1), (6)	die folgende	$(3*0)$
	(3), (4)	„	$(3*1)$
	(2), (5)	„	$(3*2)$.

Wenn nun alle Glieder auf irgend welche Weise in Perioden verteilt werden und die einzelnen Perioden wiederum in kleinere Perioden u. s. f., so behaupten wir, dass man das erreichen wird, was im vorigen Artikel versprochen wurde.

Bevor wir aber diese Auseinandersetzung selbst in Angriff nehmen, werden wir zeigen, dass der Bildung einer solchen Periode, obgleich dieselbe von den in gewisser Weise willkürlichen beiden Grössen r, ρ abhängt, doch keine Zweideutigkeit anhaftet, oder dass, wie auch diese Grössen gewählt sein mögen, doch stets dieselben Glieder in dieselbe Periode kommen (wofern nämlich vorgeschrieben ist, wieviel Glieder eine Periode enthalten soll).

Das Kriterium, dass zwei Glieder A, B in derselben Periode vorkommen, ergiebt sich daraus, dass jedes von ihnen in der Form $(\rho^{ke+\alpha})$ enthalten, oder dass $A\equiv r^{\rho^{ke+\alpha}}$, $B\equiv r^{\rho^{k'e+\alpha}}$ (mod. p) ist. Hierbei ist aber r eine primitive Wurzel der Congruenz $x^n\equiv 1$ (mod. p), ρ dagegen eine primitive Wurzel der Congruenz $x^\lambda\equiv 1$ (mod. n); vergleiche oben.

Es muss bewiesen werden, dass, wenn an Stelle der Zahlen r, ρ andere, etwa s, σ, gewählt werden, alsdann A und B in ähnlichen Formen $s^{\sigma^{le+\beta}}$, $s^{\sigma^{l'e+\beta}}$ enthalten sind.

Es sei $s^m\equiv r$ (mod. p), $\sigma^\mu\equiv\rho$ (mod. n) und $m\equiv\sigma^\zeta$ (mod. n), was möglich ist, da r, ρ primitive Wurzeln sind; m ist prim zu n, μ zu λ (Kapitel III). Nach den gehörigen Substitutionen erhält man:

$$A\equiv s^{\sigma^{\mu ke+\mu\alpha+\zeta}},\quad B\equiv s^{\sigma^{\mu k'e+\mu\alpha+\zeta}},\ \text{w. z. b. w.}$$

247.

Satz. Das Product aus zwei gleichartigen Perioden kann unabhängig von der Zahl p durch Addition gleichartiger Perioden und gegebener Zahlen gebildet werden.

(Wir nennen gleichartige Perioden solche, welche gleichviel Glieder enthalten, oder in denen die Zahl e dieselbe ist).

Beispiel. Ist $n=7$, so wird das Product aus den Perioden $(1)+(6)$ und $(2)+(5)$ $\big($wegen $(a)\cdot(b)=(a+b)\big)$ gleich $(3)+(6)+(8)+(11)$, oder es besteht aus den Perioden $(3)+(4)$ und $(1)+(6)$.

Beweis. Es sei $\frac{\lambda}{e} = f$ und die gegebenen Perioden seien $(e * \alpha)$ und $(e * \beta)$ oder die Aggregate

$$(\rho^{\alpha}) + (\rho^{\alpha+e}) + (\rho^{\alpha+2e}) + \cdots + (\rho^{\alpha+(f-1)e}) = P$$
$$(\rho^{\beta}) + (\rho^{\beta+e}) + (\rho^{\beta+2e}) + \cdots + (\rho^{\beta+(f-1)e}) = Q.$$

Das Product PQ wird aus f^2 Gliedern bestehen. Diese aber sind folgendermassen anzuordnen. Man bilde f Reihen, deren jede aus f Gliedern besteht. Die erste umfasst das Product aus P und (ρ^{β}), die zweite das Product aus P und $(\rho^{\beta+e})$, u. s. w. In der ersten Reihe nimmt den ersten Platz ein das Product, welches aus dem Gliede (ρ^{α}), den zweiten dasjenige, welches aus $(\rho^{\alpha+e})$ hervorgeht, und so die übrigen der Reihe nach weiter; in der zweiten Reihe aber werde der erste Platz dem aus dem Gliede $(\rho^{\alpha+e})$ entstehenden Producte, der zweite dem aus $(\rho^{\alpha+2e})$ entstehenden Producte u. s. w., der letzte endlich dem aus (ρ^{α}) hervorgehenden Producte zugewiesen; die dritte Reihe möge mit dem aus dem Gliede $(\rho^{\alpha+2e})$ entstehenden Gliede beginnen u. s. w., und auf das Product aus dem letzten Gliede möge folgen das Product aus dem ersten, zweiten, u. s. w. Gliede; oder wenn die aufeinanderfolgenden Glieder der Periode P mit $1, 2, 3, \ldots, z$ und diejenigen der Periode Q mit I, II, III, ..., Z bezeichnet werden, so entstehen folgende Teile von PQ:

$$\begin{array}{l} 1\cdot \mathrm{I} + 2\cdot \mathrm{I} + 3\cdot \mathrm{I} + 4\cdot \mathrm{I} + \cdots\cdot + z\cdot \mathrm{I} \\ 2\cdot \mathrm{II} + 3\cdot \mathrm{II} + 4\cdot \mathrm{II} + \cdots\cdots\cdots + 1\cdot \mathrm{II} \\ 3\cdot \mathrm{III} + 4\cdot \mathrm{III} + \cdots\cdots\cdots + 1\cdot \mathrm{III} + 2\cdot \mathrm{III} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \end{array}$$

Sodann sammle man sämtliche Glieder, welche in den einzelnen Reihen dieselbe Stelle einnehmen, zu f Ordnungen; dann behaupte ich:

1. Wenn irgend ein Glied $\equiv 1$ ist, so sind sämtliche übrigen Glieder derselben Ordnung ebenfalls $\equiv 1$.

2. Jede Ordnung, in welcher kein Glied $\equiv 1$ ist, bildet eine Periode.

Haben wir dies bewiesen, so haben wir offenbar unser Ziel erreicht.

Die allgemeine Form einer solchen Ordnung ist:

$$(\rho^{\alpha+ke} + \rho^{\beta}),\ (\rho^{\alpha+(k+1)e} + \rho^{\beta+e}),\ (\rho^{\alpha+(k+2)e} + \rho^{\beta+2e}), \ldots,\ (\rho^{\alpha+(k+f-1)e} + \rho^{\beta+(f-1)e}),$$

denn es kann für $\rho^{\alpha+(k-1)e}$ auch $\rho^{\alpha+(k+f-1)e}$ geschrieben werden, weil $ef = \lambda$ und $\rho^{\lambda} \equiv 1 \pmod{n}$ ist, und ebenso in Bezug auf die vorhergehenden. Setzt man $\rho^{\alpha+ke} + \rho^{\beta} \equiv \rho^{x} \pmod{n}$, was erlaubt ist, wenn nicht etwa $\rho^{\alpha+ke} + \rho^{\beta}$ durch n teilbar ist*), so lässt sich die Ordnung auch so darstellen:

$$(\rho^{x}),\ (\rho^{x+e}),\ (\rho^{x+2e}),\ \ldots\ (\rho^{x+(f-1)e}),$$

*) Der Satz muss ein wenig anders ausgedrückt werden, wenn n allgemein eine Potenz einer Primzahl bezeichnet; ist aber n eine Primzahl, so ist nichts zu ändern.

und dies ist offenbar die Periode $(e * \varkappa)$; ist dagegen $\rho^{\alpha+ke} + \rho^{\beta}$ durch n teilbar, so werden alle Glieder der Ordnung $\equiv (0)$ d. h. $\equiv 1$ sein.

Anmerkung. Dieser Beweis zeigt zugleich ein sehr leichtes Verfahren, das Product zu entwickeln. Einen anderen werden wir unten geben, der zwar diesen Vorzug nicht besitzt, aber seiner Einfachheit wegen nicht gering zu achten sein dürfte.

248.

Sämtliche kleineren Perioden, welche eine grössere Periode bilden, nennen wir ein **Periodensystem.** So werden die Perioden

$$(ef * \alpha),\ (ef * f + \alpha),\ (ef * 2f + \alpha),\ \ldots,\ (ef * (e-1)f + \alpha),$$

aus denen die Periode $(f * \alpha)$ zusammengesetzt ist, mit diesem Namen bezeichnet werden. Vorschriftsmässig angeordnet wird es sein, wenn die nach dem Sternchen $*$ stehenden Zahlen, wie hier α, $f+\alpha$, $2f+\alpha$, ..., in arithmetischer Progression (deren Differenz f ist) fortschreiten; gleichartig endlich werden die Systeme sein, wenn sowohl die kleineren als auch die grösseren Perioden gleichartig sind.

Satz. Wenn die Perioden zweier gleichartigen vorschriftsmässig angeordneten Systeme mit einander multipliciert werden, nämlich die erste mit der ersten, die zweite mit der zweiten, die dritte mit der dritten, u. s. w., so lässt sich die Summe aller Producte aus der grösseren Periode gleichartigen Perioden und gegebenen Zahlen zusammensetzen.

Beweis. Es seien die Systeme:

$$(ef * \alpha),\ (ef * \alpha + f),\ (ef * \alpha + 2f),\ \ldots.$$
$$(ef * \beta),\ (ef * \beta + f),\ (ef * \beta + 2f),\ \ldots.$$

Die Producte aus den einzelnen Perioden des ersten Systems und den entsprechenden Perioden des zweiten Systems bestehen nach dem vorigen Artikel aus ganzen Zahlen und gleichartigen Perioden. Geringe Aufmerksamkeit auf die Entstehung dieser Perioden aber zeigt, dass, wenn $(ef * \alpha) \cdot (ef * \beta)$ aus der ganzen Zahl N und den Perioden $(ef * A)$, $(ef * B)$, $(ef * C)$, ... besteht, alsdann das Product

$(ef * \alpha + f) \cdot (ef * \beta + f)$ aus N und den Perioden $(ef * A + f)$, $(ef * B + f)$, $(ef * C + f)$, ...

$(ef * \alpha + 2f) \cdot (ef * \beta + 2f)$ aus N und den Perioden $(ef * A + 2f)$, $(ef * B + 2f)$, $(ef * C + 2f)$, ...

und allgemein

$(ef * \alpha + \mu f) \cdot (ef * \beta + \mu f)$ aus N und den Perioden $(ef * A + \mu f)$, $(ef * B + \mu f)$, $(ef * C + \mu f)$, ...

besteht. Hieraus geht unmittelbar hervor, dass die Summe aller Perioden gleich

$$eN + (f * A) + (f * B) + (f * C) + \cdots$$

ist, w. z. b. w.

Auch dieser Beweis giebt ein Verfahren an die Hand, jene Summe zu finden.

249.

Es ist leicht, diesen Satz noch zu verallgemeinern, nämlich dahin, dass, wenn man beliebig viele vorschriftsmässig angeordnete gleichartige Systeme hat und aus den ersten, zweiten, u. s. w. Perioden Producte gebildet werden, die Summe aller dieser Producte aus Zahlen und grösseren Perioden besteht. Wenn alle diese Systeme als gleich vorausgesetzt werden, so wird die Summe irgend welcher Potenzen sämtlicher Perioden aus Zahlen und der grösseren Periode gleichartigen Perioden bestehen. Schon hieraus ist das Ziel dieser Untersuchung ersichtlich. Es sei $\lambda = efgh \ldots$; man zerlege sämtliche eigentlichen Wurzeln in e Perioden $A, A', A'', \ldots$, jede von diesen wiederum in f: $B, B', B'', \ldots$, jede einzelne von diesen in g: $C, C', C'', \ldots$ Nun ist die Summe aller Perioden gegeben, dieselbe ist nämlich $\equiv -1$. Nach dem, was wir eben auseinandergesetzt haben, sind aber auch

$$(A)^2 + (A')^2 + (A'')^2 + (A''')^2 + \cdots$$
$$(A)^3 + (A')^3 + (A'')^3 + (A''')^3 + \cdots$$

u. s. w.

gegeben. Demnach lässt sich hieraus nach Artikel 244 eine Congruenz e^{ten} Grades finden, deren Wurzeln $A, A', A'', \ldots$ sind. Werden nun diese als bekannt vorausgesetzt, so zerlege man jede Periode in kleinere, nämlich

$$\begin{array}{llll} A & \text{in } B, & B', & B'', \ldots \\ A' & \text{in } B^{(n)}, & B^{(n+1)}, & B^{(n+2)}, \ldots \\ A'' & \text{in } B^{(2n)}, & B^{(2n+1)}, & B^{(2n+2)}, \ldots \end{array}$$

u. s. w.

Dann ist also $B + B' + B'' + \cdots \equiv A$ gegeben. Nun bestehen aber

$$(B)^2 + (B')^2 + (B'')^2 + \cdots$$
$$(B)^3 + (B')^3 + (B'')^3 + \cdots$$

u. s. w.

aus Einheiten und den Perioden $A, A', A'', \ldots$ Daher werden $B, B', B'', \ldots$ gegeben durch eine Congruenz f^{ten} Grades, aus der sie gefunden werden können; und auf ähnliche Weise können die Perioden, aus denen $A', A'', \ldots$ bestehen, gefunden werden. Es wird aber jeder hiernach einsehen, dass auf ganz analoge Weise jede Periode in kleinere zerlegt werden kann, bis man zu den Wurzeln selbst gelangt.

250.

Bei der Anwendung dieser Regeln aber tritt eine Schwierigkeit auf, die wir beseitigen müssen. Da nämlich jede Congruenz mehrere Wurzeln hat, müssen wir zusehen, welches Zeichen einer jeden beizulegen ist, um sie von einander richtig unterscheiden zu können. Da die Bedeutung der Perioden von den Zahlen r, ρ abhängt, die nach Belieben angenommen werden können, so muss notwendig auch jener Bedeutung etwas Willkürliches anhaften. Die Zahl ρ allerdings muss gleich von Anfang an festgestellt werden. Das Wesen unserer Methode beruht hauptsächlich darauf, dass wir aus grösseren Perioden kleinere ableiten. Dies lässt sich aber ohne die gehörige Anordnung der Perioden, eine Anordnung, die wir durch die Bezeichnungen erhalten haben, nicht ausführen. Daher müssen wir suchen, alle Perioden, sobald sie gefunden sind, durch die ihnen zukommenden Zeichen von einander zu unterscheiden.

Es sei die Periode A mit $(e * \alpha)$ bezeichnet und in die f Perioden B, C, D, ... zerlegt, die wir bestimmen sollen. Offenbar wird eine jede in einer solchen Form wie $(ef * ke + \alpha)$ enthalten sein; ich behaupte aber, dass für irgend eine derselben B die Zahl k willkürlich angenommen und daraus die Reihenfolge der übrigen abgeleitet werden kann.

Es sei R irgend eine primitive Wurzel der Congruenz $x^n \equiv 1$, und es bestehe B aus den Gliedern $R^\mu + R^\nu + \cdots$; es sei ferner $\frac{1}{\mu}\rho^{ke+\alpha} \equiv \frac{1}{v}$ (mod. n) und es werde, da der Wert von r willkürlich ist (wofern nur A das Zeichen $(e * \alpha)$ erhält, was offenbar von selbst der Fall ist), $r \equiv R^v$ (mod. p) gesetzt. Dann ist somit das erste Glied von $B: r^{\rho^{ke+\alpha}}$ und B kann mit $(ef * ke + \alpha)$ bezeichnet werden. Hätten wir an Stelle von R^μ das Glied R^ν betrachtet, so würden wir einen anderen Wert von r erhalten haben; man sieht aber leicht, dass für irgend eine Wurzel ρ die Wurzel r $\frac{\lambda}{ef}$ verschiedene Werte haben kann.

251.

Wir wollen nun sehen, wie man aus der Bestimmung einer Periode die übrigen durch ihre Zeichen unterscheiden kann. Zu diesem Zwecke aber muss man eine andere Methode, um die übrigen Wurzeln zu finden, suchen; denn insoweit die übrigen, wie A selbst, Wurzeln irgend einer Congruenz sind, ist keine Reihenfolge unter ihnen ersichtlich. Nehmen wir an, dass A mit $(ef * 0)$ bezeichnet sei, so folgt aus dem Vorhergehenden, dass

A^2 von der Form $M + N(ef * 0) + O(ef * 1) + P(ef * 2) + \cdots$
A^3 von der Form $M' + N'(ef * 0) + O'(ef * 1) + P'(ef * 2) + \cdots$
. . . .
A^{ef-1} von der Form $M^* + N^*(ef * 0) + O^*(ef * 1) + P^*(ef * 2) + \cdots$

ist. Hierzu tritt die Congruenz:

$$(ef * 0) + (ef * 1) + (ef * 2) + \cdots + (ef * ef - 1) \equiv -1.$$

Man hat also $ef - 1$ lineare Congruenzen und ebenso viele unbekannte Grössen, die somit durch Elimination bestimmt werden können.

Anmerkung. Es kann der Fall eintreten, wo die unbekannten Grössen durch Ausdrücke von der Art wie $\frac{V}{W_p}$ gegeben werden; wie man aber dieser Schwierigkeit abhelfen kann, werden wir später zeigen. Hier wollen wir uns nicht damit aufhalten, da dieser Fall nur sehr selten vorkommen kann.

252.

Dies möge im Allgemeinen über die Auflösung der reinen Congruenzen genügen. Vorübergehend wird später noch manches über sie gesagt werden; besonders lässt sich vieles aus der Auflösung der reinen Gleichungen hierauf anwenden, worauf wir an der gehörigen Stelle aufmerksam zu machen nicht versäumen werden. Wir fügen noch ein **Beispiel** hinzu, durch dessen Vergleichung mit den gegebenen Regeln den minder Geübten alles klarer werden wird.

Es sei $n = 31$, $p = 311$ oder es seien die Wurzeln der Congruenz $x^{31} - 1 \equiv 0 \pmod{311}$ zu suchen. Man hat zuerst eine primitive Wurzel der Congruenz $y^{30} - 1 \equiv 0 \pmod{31}$ zu suchen; eine solche ist $y \equiv 3$. Wir setzen daher $\rho = 3$ und zerlegen sämtliche primitiven Wurzeln der gegebenen Congruenz zunächst in fünf Perioden, nämlich:

$$\begin{aligned}
(5 * 0) &= (\ 1) + (26) + (25) + (30) + (\ 5) + (\ 6) \\
(5 * 1) &= (\ 3) + (16) + (13) + (28) + (15) + (18) \\
(5 * 2) &= (\ 9) + (17) + (\ 8) + (22) + (14) + (23) \\
(5 * 3) &= (27) + (20) + (24) + (\ 4) + (11) + (\ 7) \\
(5 * 4) &= (19) + (29) + (10) + (12) + (\ 2) + (21).
\end{aligned}$$

Nach den erforderlichen Rechnungen findet man die Summe der Perioden $\equiv -1$, der Quadrate $\equiv 25$, der Kuben $\equiv 26$, der Biquadrate $\equiv 249$, der fünften Potenzen $\equiv 564$.

Demnach sind die Perioden die Wurzeln der Congruenz:

$$x^5 + x^4 - 12x^3 - 21x^2 + x + 5 \equiv 0.$$

Ferner aber findet man:

$$\begin{aligned}
(5 * 0)^2 &\equiv \ 6 + \ 2(5 * 0) + \quad * \quad + \quad * \quad + 2(5 * 3) + \ (5 * 4) \\
(5 * 0)^3 &\equiv 12 + 15(5 * 0) + \ 4(5 * 1) + \ 3(5 * 2) + \ 6(5 * 3) + \ 6(5 * 4) \\
(5 * 0)^4 &\equiv 90 + 60(5 * 0) + 28(5 * 1) + 26(5 * 2) + 49(5 * 3) + 38(5 * 4),
\end{aligned}$$

und hieraus durch Elimination:

$$
\begin{aligned}
5(5*1) &\equiv 3(5*0)^4 - (5*0)^3 - 33(5*0)^2 - 24(5*0) + 15\\
5(5*2) &\equiv -2(5*0)^4 - (5*0)^3 + 22(5*0)^2 + 31(5*0)\\
5(5*3) &\equiv (5*0)^4 - 2(5*0)^3 + 11(5*0)^2 - 12(5*0) - 20\\
5(5*4) &\equiv -2(5*0)^4 + 4(5*0)^3.
\end{aligned}
$$

Eine Wurzel der gefundenen Congruenz ist aber $\equiv 17$; setzt man daher $(5*0) \equiv 17$, so wird:

$$(5*1) \equiv 183,\quad (5*2) \equiv 263,\quad (5*3) \equiv 91,\quad (5*4) \equiv 67.$$

Nun zerlege man die einzelnen gefundenen Perioden wiederum in je drei, nämlich:

$(5*0)$ in $(15*0)$, $(15*5)$, $(15*10)$ oder in $(1)+(30)$, $(26)+(5)$, $(25)+(6)$
$(5*1)$ in $(15*1)$, $(15*6)$, $(15*11)$ oder in $(3)+(28)$, $(16)+(15)$, $(13)+(18)$
u. s. w.

Nimmt man an, dass die Perioden, in welche

$(5*0)$ zerlegt ist, Wurzeln der Congruenz $x^3 + Ax^2 + Bx + C \equiv 0$ seien,
$(5*1)$ „ „ „ „ „ $x^3 + A'x^2 + B'x + C' \equiv 0$ „
$(5*2)$ „ „ „ „ „ $x^3 + A''x^2 + B''x + C'' \equiv 0$ „
u. s. w.,

so ist:

$$
\begin{aligned}
A &\equiv -(5*0), & B &\equiv (5*0) + (5*3), & C &\equiv -2-(5*4)\\
A' &\equiv -(5*1), & B' &\equiv (5*1) + (5*4), & C' &\equiv -2-(5*0)\\
&\text{u. s. w.} & &\text{u. s. w.} & &\text{u. s. w.}
\end{aligned}
$$

Daher sind

$(15*0)$, $(15*5)$, $(15*10)$ Wurzeln der Congruenz $x^3 - 17x^2 + 108x - 69 \equiv 0$
$(15*1)$, $(15*6)$, $(15*11)$ „ $x^3 + 128x^2 - 61x - 19 \equiv 0$
$(15*2)$, $(15*7)$, $(15*12)$ „ $x^3 + 48x^2 - 31x + 126 \equiv 0$
$(15*3)$, $(15*8)$, $(15*13)$ „ $x^3 - 91x^2 - 37x + 46 \equiv 0$
$(15*4)$, $(15*9)$, $(15*14)$ „ $x^3 - 67x^2 + 19x - 93 \equiv 0.$

Hier aber hat man:

$$
\begin{aligned}
(15*0)^3 - 3(15*0) &\equiv (15*1)\\
(15*1)^3 - 3(15*1) &\equiv (15*2)
\end{aligned}
$$
u. s. w.

Setzt man daher eine der Wurzeln der ersten Congruenz, etwa 10, gleich (15 * 0), so erhält man hieraus:

$$\begin{array}{lll}
(15 * 0) \equiv 10, & (15 * 5) \equiv -116, & (15 * 10) \equiv 123 \\
(15 * 1) \equiv 37, & (15 * 6) \equiv 50, & (15 * 11) \equiv 96 \\
(15 * 2) \equiv -151, & (15 * 7) \equiv 139, & (15 * 12) \equiv -36 \\
(15 * 3) \equiv -39, & (15 * 8) \equiv 28, & (15 * 13) \equiv 102 \\
(15 * 4) \equiv -112, & (15 * 9) \equiv 98, & (15 * 14) \equiv 81.
\end{array}$$

Nimmt man endlich die Glieder, welche diese einzelnen Perioden bilden, so sind:

(1), (30) Wurzeln der Congruenz $x^2 - (15 * 0)x + 1 \equiv 0$
(3), (28) „ „ „ $x^2 - (15 * 1)x + 1 \equiv 0$
u. s. w.

Die Wurzeln der ersten Congruenz sind 126 und 195; diese werden somit primitive Wurzeln der Congruenz $x^{31} \equiv 1$ sein, und aus ihnen können die übrigen ohne Mühe abgeleitet werden.

Die Lehre von den Resten.

II.

Allgemeine Untersuchungen über die Congruenzen.

330.*)

Was wir in den vorhergehenden Abschnitten über die Congruenzen mitgeteilt haben, betrifft nur die einfachsten Fälle und ist meistens durch specielle Methoden gefunden worden. In diesem Abschnitte wollen wir versuchen, die Theorie der Congruenzen, soweit dies wenigstens zur Zeit möglich ist, auf höhere Prinzipien zurückzuführen, ungefähr in ähnlicher Weise, wie man die Theorie der Gleichungen betrachtet, mit welcher, wie wir schon oft hervorgehoben haben, eine hervorragende Analogie besteht. Da nun alle algebraischen Congruenzen mit nur einer Unbekannten auf die Form

$$X \equiv 0,$$

wo X eine algebraische, keine Brüche enthaltende Function der Unbekannten x ist, zurückgeführt werden können, so werden insbesondere derartige Functionen zu betrachten sein.

331.

Wenn P, Q Functionen der Unbestimmten x von der Form

$$A + Bx + Cx^2 + Dx^3 + \cdots$$
$$H + Jx + Kx^2 + Lx^3 + \cdots$$

(und solche sollen im Folgenden stets unter der einfachen Bezeichnung von Functionen verstanden werden) und in jeder von ihnen die Coefficienten gleichhoher Potenzen von x nach irgend welchem Modul congruent sind, so sollen die Functionen nach diesem Modul congruent genannt werden. Offenbar aber werden congruente Functionen, wenn für die Unbestimmte gleiche oder congruente Werte genommen werden, congruente Werte erhalten. Was wir in den Abschnitten I und II von den Zahlen bewiesen haben, gilt in den meisten Fällen auch von den Functionen. Ist

*) Vgl. das Vorwort des Herausgebers und die nachfolgenden Bemerkungen.

z. B. $P \equiv P'$, $Q \equiv Q'$, $R \equiv R'$, ..., so ist offenbar auch $P + Q + R + \cdots \equiv P' + Q' + R' + \cdots$; $P - Q \equiv P' - Q'$; $PQ \equiv P'Q'$; $PQR \cdots \equiv P'Q'R' \ldots$

Die Beweise sind sehr leicht und lassen sich in analoger Weise führen, wie im ersten Abschnitt.

Ist $PQ \equiv R$, so werden wir die Function Q durch $\frac{R}{P}$ mit beigesetztem Modul bezeichnen und werden sagen, Q sei der Quotient, wenn R durch P nach diesem Modul geteilt wird. Offenbar aber können an Stelle von Q sämtliche dieser Function congruente Functionen genommen werden, die wir alle als einen einzigen Wert betrachten werden. Weiter unten aber werden wir zeigen, in welchen Fällen ein solcher Quotient mehrere (d. h. incongruente) Werte erhalten kann.

332.

Wenn der Modul eine Primzahl ist und der Divisor Q nur ein einziges Glied, Hx^h, enthält, dessen Coefficient H durch den Modul nicht teilbar ist, d. h. wofern H nicht $\equiv 0$ ist, so kann der Quotient nicht mehrere Werte besitzen. Denn wenn $QA \equiv P$ und $QB \equiv P$ wäre, so würde $Q(A-B) \equiv 0$ sein. Ist nun

$$Q \equiv \cdots + Hx^h + Jx^{h+1} + \cdots,$$

so dass H durch p nicht teilbar ist, und

$$A - B \equiv Lx^l + Mx^{l+1} + \cdots,$$

so dass L durch p nicht teilbar ist (eine solche Form wird aber $A - B$ haben, da wir annehmen, dass A nicht $\equiv B$ ist), so würde $Q(A-B) \equiv HLx^{h+l} + \cdots \equiv 0$ sein, was absurd ist, da HL nicht $\equiv 0$ ist.

Man kann nun leicht Regeln angeben, um die Function P durch Q, wofern dies möglich ist, zu teilen. Ist

$$P \equiv ax^\alpha + bx^{\alpha+1} + cx^{\alpha+2} + \cdots + kx^\varkappa$$
$$Q \equiv mx^\mu + nx^{\mu+1} + qx^{\mu+2} + \cdots + tx^\tau,$$

so dass sich a, k, m, t durch den Modul nicht teilen lassen, so muss sein α nicht $< \mu$, $\varkappa$ nicht $< \tau$. Die Division lässt sich aber auf ähnliche Weise ausführen wie in der elementaren Arithmetik, wofern man nur immer für den Quotienten eine ganze Zahl nimmt; der Quotient wird nämlich immer die Form $\frac{r}{m}$ haben, was nach dem Modul bestimmt werden muss. Wenn nun, nachdem $\varkappa + \mu - \alpha - \tau + 1$ Glieder gefunden sind, ein Rest bleibt, welcher von der Form

$$Ax^{\varkappa+\mu-\tau+1} + Bx^{\varkappa+\mu-\tau+2} + \cdots + Cx^\varkappa$$

sein wird, und nicht alle Coefficienten $A, B, C, \ldots \equiv 0$ sind, so lässt sich P durch Q nicht teilen.

Übrigens ist klar, dass die Division auch mit den Gliedern, welche die meisten Dimensionen haben, $kx^{\varkappa}$, tx^{τ}, hätte begonnen werden können; die Rechnung wird erleichtert, wenn Q auf die Form gebracht wird:

$$mx^{\mu}(1 + qx + rx^2 + \cdots),$$

wonach, wenn $mv \equiv 1$ gesetzt wird,

$$\frac{P}{Q} \equiv \frac{vP : x^{\mu}}{1 + qx + \cdots}$$

ist; hierauf kann aber die Division nach den gewöhnlichen Methoden ausgeführt werden.

333.

Satz. Ist $x \equiv a$ eine Wurzel der Congruenz $\xi \equiv 0$, so lässt sich ξ durch $x - a$ nach dem Modul der Congruenz teilen.

Beweis. Denn wenn sich ξ nicht teilen liesse, so würde $\xi \equiv (x - a)\xi' + b$ sein, so dass b durch den Modul nicht geteilt werden könnte. Setzt man nun $x \equiv a$, so wird $\xi \equiv 0$ nach Voraussetzung, daher $(x - a)\xi' + b \equiv 0$; dann ist aber auch $(x - a)\xi' \equiv 0$ und somit notwendig $b \equiv 0$.

334.

Aufgabe. Wenn zwei Functionen gegeben sind, so soll man ihren gemeinschaftlichen Teiler (von der höchsten Dimension) nach einem gegebenen Modul finden.

Auflösung. Die Functionen seien A und B. Es besitze A ebensoviele oder mehr Dimensionen als B. Man dividiere A durch B; geht die Division auf, so ist B der gesuchte gemeinschaftliche Teiler. Bleibt ein Rest C, so wird dieser von niedrigerer Dimension sein als B. Es sei also:

$$A \equiv aB + C, \quad B \equiv bC + D, \quad C \equiv cD + E, \cdots,$$

so dass $A, B, C, D, \ldots, a, b, c, \ldots$ Functionen sind und die Dimensionen der Functionen $A, B, C, D, \ldots$ eine abnehmende Reihe bilden. Wenn nun schliesslich irgend eine Division aufgeht, z. B. $D \equiv dE$ ist, so wird der letzte Divisor der gesuchte gemeinschaftliche Teiler sein; geht aber keine auf, so wird man schliesslich zu einem Rest kommen, welcher keine Dimension besitzt, d. h. zu einer Zahl; in diesem Falle aber haben die Functionen A, B keinen gemeinschaftlichen Teiler.

Beweis. Wenn der Divisor E die vorhergehende Function ohne Rest teilt, so wird sie, wie leicht ersichtlich, alle vorhergehenden teilen; somit wird E ein gemeinschaftlicher Teiler von A, B sein. Dies ist der erste Teil des Satzes. Gäbe es aber einen Divisor von höherer Dimension, etwa E', so würde dieser wegen $C \equiv A - aB$ auch C und aus ähnlichem Grunde auch D u. s. w. und somit E teilen, d. h. eine Function von höherer Dimension würde in einer Function von niedrigerer Dimension aufgehen. Dies ist aber absurd, und daher die zweite Behauptung erwiesen.

Hieraus geht auch hervor, dass man, wenn es einen gemeinschaftlichen Divisor von irgend einer Dimension giebt, nicht zu einem Rest von keiner Dimension gelangen kann, denn sonst würde eine Function von keiner Dimension durch eine Function von irgend einer Dimension geteilt werden, was absurd ist.

335.

Satz. Wenn A und B nach dem Modul p unter einander prime Functionen sind und A von der α^{ten}, B von der β^{ten} Dimension ist, so lassen sich Functionen P, Q von Dimensionen, welche bezüglich $<\beta$, $<\alpha$ sind, derart finden, dass

$$PA + QB \equiv 1 \pmod{p}$$

ist.

Beweis. Denn in diesem Falle ist:

$$A \equiv aB + C,\ B \equiv bC + D,\ \ldots,\ K \equiv kL + M$$

derart, dass die Dimensionen der Functionen $A, B, C, D, \ldots, K, L, M$ beständig abnehmen und M von keiner Dimension ist. Bildet man nun die Reihen:

$$a,\ a',\ a'',\ a''',\ \ldots,\ a^{(\varkappa)}$$
$$1,\ b,\ b',\ b'',\ \ldots,\ b^{(\varkappa-1)}$$

derart, dass

$$a' \equiv ba + 1,\ a'' \equiv ca' + a,\ a''' \equiv da'' + a',\ \ldots$$
$$b' \equiv cb + 1,\ b'' \equiv db' + b,\ b''' \equiv cb'' + b',\ \ldots$$

ist, so wird, wie leicht ersichtlich

$$A - aB \equiv + C,\ bA - a'B \equiv -D,\ b'A - a''B \equiv + E,\ \ldots$$

sein, und schliesslich:

$$b^{(\varkappa-1)} A - a^{(\varkappa)} B \equiv \pm M.$$

Ist nun $\dfrac{1}{\pm M} \equiv \mu$, so wird, wenn man $P \equiv \mu b^{(\varkappa-1)}$, $Q \equiv -\mu a^{(\varkappa)}$ setzt

$$PA + QB \equiv 1.$$

Ferner aber ist klar, dass

die Dimension von $B +$ der Dimension von $a =$ der Dimension von A
„ „ „ $C +$ „ „ „ $b =$ „ „ „ B
. . . .
die Dimension von $L +$ der Dimension von $k =$ der Dimension von K

ist. Mithin ist:

Dimension von $L +$ Summe der Dimensionen von $a, b, c \ldots, k =$ Dimension von A.

Offenbar aber ist die Dimension von $a^{(\varkappa)}$ und somit auch die Dimension von $Q =$ Summe der Dimensionen von $a, b, c, \ldots$ d. h. $= \alpha -$ Dimension L. Mithin:

Dimension von $P = \beta -$ Dimension von L. W. z. b. w.

336.

Hieraus aber folgt, dass, wenn M der gemeinschaftliche Teiler höchster Dimension von den Functionen A, B ist, stets gesetzt werden kann:

$$AP + BQ \equiv M.$$

Beispiele für den vorstehenden Satz lasse ich der Kürze wegen fort, doch mögen es die Leser nicht unterlassen, sich durch solche eine gewisse Fertigkeit in der Behandlung derartiger Aufgaben zu verschaffen. Übrigens verlohnt es sich darauf hinzuweisen, dass der vorstehende Satz auch von absolut genommenen Functionen gilt, sofern deren Coefficienten rationale Zahlen sind. Dies geht aus der Art des Beweises von selbst hervor. Doch können wir uns damit nicht aufhalten. Ähnliches wird der Leser, auch ohne darauf hingewiesen zu werden, im Folgenden bemerken.

Wenn A weder mit B noch mit C einen gemeinschaftlichen Teiler von irgend einer Dimension hat, so wird sie auch mit dem Producte BC keinen gemeinschaftlichen Teiler haben. Denn ist

$$PA + QB \equiv 1, \text{ so wird } PAC + QBC \equiv C \text{ sein.}$$

Wenn nun A mit BC einen gemeinschaftlichen Teiler M hätte, so würde derselbe im Widerspruche mit der Voraussetzung auch in C aufgehen. Hiernach wird allgemein, wenn die Function A zu den Functionen B, C, D, ... prim ist, dieselbe auch zu ihrem Producte prim sein.

Wenn A, B, C, D, ... keinen allen gemeinschaftlichen Teiler haben, so kann

$$PA + QB + RC + SD + \cdots \equiv 1$$

gemacht werden.

Ist M der Divisor höchster Dimension von A und B, M' der von M und C, M'' der von M' und D, u. s. w., so ist offenbar das letzte Glied dieser Reihe von keiner Dimension (nach Voraussetzung). Daher kann man setzen:

$$aA + bB \equiv M, \quad mM + cC \equiv M', \quad m'M' + dD \equiv M'', \ldots$$

und führt man die Substitutionen aus, so ergiebt sich die Richtigkeit des Satzes.

337.

Satz. Sind die Functionen A, B, C, ... nach dem Modul p zu einander prim (haben also keine zwei von ihnen einen gemeinschaftlichen Teiler) und ist die Function M nach demselben Modul durch jede einzelne teilbar, so ist sie auch durch das Product aller teilbar.

Beweis. Es kann gesetzt werden $PA + QB \equiv 1$, daher ist:

$$\frac{M}{A}Q + \frac{M}{B}P \equiv \frac{M}{AB}.$$

Da nun C zu AB prim ist, so wird auch M durch ABC und aus ähnlichem Grunde durch $ABCD$ u. s. w. teilbar sein.

338.

Wenn die Congruenz $\xi \equiv 0$ die Wurzeln $x \equiv a$, $x \equiv b$, $x \equiv c, \ldots$ hat, so lässt sich ξ durch das Product aus $(x - a)$, $(x - b)$, $(x - c), \ldots$ teilen. Denn da $a, b, c, \ldots$ zu einander incongruent vorausgesetzt werden, so sind die Functionen $x - a$, $x - b$, $x - c, \ldots$ prim zu einander, und da ξ durch jede einzelne teilbar ist, so wird sie auch durch das Product aus allen teilbar sein. Hieraus geht hervor, dass die Anzahl der Wurzeln die Dimension der Congruenz nicht übersteigen kann; dies ist der von uns versprochene Beweis dieses Satzes.

Aber zugleich ersieht man hieraus, dass die Lösung der Congruenzen nur einen Teil einer viel höheren Untersuchung bildet, nämlich der Untersuchung über die Zerlegung der Functionen in Factoren. Es ist klar, dass die Congruenz $\xi \equiv 0$ keine reellen Wurzeln hat, wenn ξ keine Factoren von einer Dimension besitzt; aber es hindert nichts, dass ξ in Factoren von zwei, drei oder mehr Dimensionen zerlegt werden kann, wonach jener gewissermassen imaginäre Wurzeln zugeschrieben werden können. In der That hätten wir, wenn wir uns einer ähnlichen Freiheit, wie sie neuere Mathematiker sich erlaubt haben, bedienen und derartige imaginäre Grössen einführen wollten, alle unsere nachfolgenden Untersuchungen unvergleichlich zusammenziehen können; nichtsdestoweniger haben wir es vorgezogen, Alles aus den Prinzipien abzuleiten.*)

339.

Die Functionen werden nach einem bestimmten Modul prim genannt, wenn sie durch keine Functionen niedrigeren Grades nach diesem Modul sich teilen lassen.

So sind z. B. alle Functionen von einer Dimension prim; die Functionen von zwei Dimensionen aber sind entweder prim oder aus zwei primen Functionen von einer Dimension zusammengesetzt; mithin wird ξ eine Primfunction von zwei Dimensionen sein, wenn die Congruenz $\xi \equiv 0$ keine reellen Wurzeln besitzt. So ist z. B. die Function $x^2 + x + 1$ für den Modul 5 prim, weil

$$x^2 + x + 1 \equiv (x - 2)^2 - 3 \pmod{5}$$

und 3 quadratischer Nichtrest von 5 ist.

Diese Primfunctionen aber erheischen vor allen unsere Aufmerksamkeit. Denn obwohl andere als solche ersten Grades zur Auffindung der reellen Wurzeln nicht dienen können, so empfiehlt sich doch eine ausführlichere Betrachtung derselben sowohl wegen ihrer ausgezeichneten Eigenschaften als auch wegen anderer aus ihnen abzuleitender herrlicher Wahrheiten.

---

*) Vielleicht werden wir bei anderer Gelegenheit unsere Ansicht hierüber ausführlicher darlegen.

340.

Satz. Jede beliebige Function ist entweder eine Primfunction oder aus Primfunctionen zusammengesetzt, und im letzteren Falle lässt sie sich nur auf eine einzige Weise aus Primfunctionen zusammensetzen.

Beweis. Ist nämlich die gegebene Function A nicht prim, so wird sie sich durch eine andere B von niedrigerer Dimension teilen lassen. Ist B keine Primfunction, so wird sie durch eine andere C von niedrigerem Grade teilbar sein, und indem man so fortfährt erhellt, dass man schliesslich zu einer Primfunction gelangen wird, weil ja sonst diese Reihe unendlich sein würde, was absurd ist, da die Dimensionen beständig abnehmen. Wenn nun die letzte Primfunction L ist, so wird diese in allen vorhergehenden aufgehen. Daher ist $A \equiv LA'$, und A' ist von niedrigerer Dimension als A. Da nun wiederum $A' \equiv L'A''$, u. s. w. wird, so wird man offenbar schliesslich zu einer Primfunction gelangen, und daher wird A dem Producte aus den Primfunctionen L, L', L'', ... congruent.

Wenn nun auch $A \equiv MM'M'' \ldots$ wäre, und nicht alle Functionen L, L', L'', ... mit den M, M', M'' ... identisch wären, so lasse man diejenigen, welche beiden Reihen gemeinschaftlich sind, weg. Bleiben die Functionen λ, λ', λ'', ...; μ, μ', μ'', ... übrig, so wird μ zu λ, λ', λ'', ... und daher auch zu ihrem Producte $\lambda\lambda'\lambda'' \ldots$ prim sein. Trotzdem müsste sein:

$$\lambda\lambda'\lambda'' \ldots \equiv \mu\mu'\mu'' \ldots, \text{ d. h. } \frac{\lambda\lambda'\lambda'' \ldots}{\mu} \equiv \mu'\mu'' \ldots,$$

was absurd ist.

341.

Die Hauptaufgabe dieser Untersuchungen besteht darin, die Anzahl der Primfunctionen jeder Dimension zu bestimmen. Da nämlich für einen bestimmten Modul die Anzahl aller verschiedenen (incongruenten) Functionen jeden Grades beschränkt ist, von diesen aber die einen aus Primfunctionen von niedrigerem Grade zusammengesetzt, die andern selbst prim sind, so ist auch die Anzahl dieser endlich. Eine strenge Entwicklung dieses Gegenstandes ist ziemlich schwierig; wir werden mit den einfacheren Fällen beginnen.

Setzt man den Modul gleich p, so ist die Anzahl aller verschiedenen Functionen n^{ten} Grades von der Form

$$x^n + Ax^{n-1} + Bx^{n-2} + Cx^{n-3} + \cdots$$

gleich p^n. Denn die Anzahl der Coefficienten A, B, C, ... ist gleich n, und da jeder unabhängig von den übrigen $\equiv 0, 1, 2, 3, \ldots, p-1$ (mod. p) sein kann, so folgt aus der Combinationslehre, dass man p^n verschiedene Combinationen hat; diese werden daher den Complex aller verschiedenen Functionen dieses Grades bestimmen.

So giebt es p verschiedene Functionen von einer Dimension, nämlich x, $x+1$, $x+2$, bis zu $x+p-1$; p^2 verschiedene Functionen von zwei Dimensionen u. s. w.

342.

Schon oben haben wir darauf hingewiesen, dass sämtliche Functionen ersten Grades für prim zu halten sind; wenn wir uns daher, was zu unserm Zwecke ausreicht, auf diejenigen Functionen beschränken, deren höchstes Glied den Coefficienten 1 hat, so giebt es p Functionen ersten Grades oder von einer Dimension.

Alle Functionen zweiten Grades sind entweder aus zwei Functionen ersten Grades zusammengesetzt oder prim. Nun weiss man aus der Theorie der Combinationen, dass p verschiedene Dinge mit Wiederholungen auf $\frac{p(p+1)}{1\cdot 2}$ verschiedene Weisen zu zweien combiniert werden können; daher werden ebenso viele aus zwei Primfunctionen von einer Dimension zusammengesetzte Functionen und somit $p^2-\frac{p(p+1)}{1\cdot 2}=\frac{1}{2}(p^2-p)$ Primfunctionen von zwei Dimensionen existieren.

In ähnlicher Weise sind von allen Functionen dritten Grades, deren Anzahl p^3 ist, diejenigen auszuschliessen, welche aus drei Primfunctionen von einer Dimension zusammengesetzt sind und deren Anzahl $\frac{p(p+1)(p+2)}{1\cdot 2\cdot 3}$ ist, und ferner diejenigen, welche aus einer Primfunction von einer Dimension und einer andern von zwei Dimensionen zusammengesetzt sind und deren Anzahl $p\cdot\frac{1}{2}(p^2-p)$ ist. Lässt man diese weg, so bleiben $\frac{1}{3}(p^3-p)$ übrig; so viele Primfunctionen von drei Dimensionen giebt es also. Offenbar kann man auf diese Weise stets fortfahren.

343.

Um aber diese Operationen leichter zu erledigen und zugleich zur Entwicklung des allgemeinen Gesetzes den Weg zu bahnen, wollen wir die Sache allgemein betrachten. Der Kürze wegen bezeichnen wir mit (1) die Anzahl der Primfunctionen einer Dimension, mit (2) die Anzahl der Primfunctionen von zwei Dimensionen u. s. w., mit (1^2) die Anzahl der aus zwei Primfunctionen von einer Dimension zusammengesetzten Functionen u. s. w., allgemein mit $(1^\alpha 2^\beta 3^\gamma\ldots)$ die Anzahl aller Functionen, welche aus Primfunctionen zusammengesetzt sind, und zwar aus α solchen von einer Dimension, aus β solchen von zwei, aus γ solchen von drei Dimensionen u. s. w., deren Dimension somit $\alpha+2\beta+3\gamma+\cdots$ ist. Dann erhellt aus dem Vorhergehenden und der Theorie der Combinationen, dass

$$(1^\alpha 2^\beta 3^\gamma 4^\delta\ldots)=(1^\alpha)(2^\beta)(3^\gamma)(4^\delta)\ldots,$$

$$(1^\alpha) = \frac{(1)\,[(1)+1]\,[(1)+2]\,[(1)+3]\cdots[(1)+\alpha-1]}{1\cdot 2\cdot 3\cdot 4\cdots\alpha}$$

oder allgemein

$$(a^\alpha) = \frac{(a)\,[(a)+1]\,[(a)+2]\,[(a)+3]\cdots[(a)+\alpha-1]}{1\cdot 2\cdot 3\cdot 4\cdots\alpha}$$

ist. Endlich ist klar, dass, wenn man alle verschiedenen Arten, die Zahl n aus den Zahlen 1, 2, 3, ... durch Addition zusammenzusetzen, welche Arten mit $\alpha\cdot 1 + \beta\cdot 2 + \gamma\cdot 3 + \cdots$ bezeichnet werden mögen, sammelt, die Summe aller dieser Ausdrücke $(1^\alpha 2^\beta 3^\gamma \ldots)$ gleich der Anzahl aller Functionen von n Dimensionen, d. h. gleich p^n, ist. So ist z. B.

$$\begin{aligned} p &= (1)\\ p^2 &= (1^2) + 2\\ p^3 &= (1^3) + (1\cdot 2) + (3)\\ p^4 &= (1^4) + (1^2\cdot 2) + (1\cdot 3) + (2^2) + (4)\end{aligned}$$

u. s. w.

Man sieht, dass in den Ausdruck p^n ausser den Grössen (1), (2), (3), ... auch der folgende (n) eingeht, woraus hervorgeht, auf welche Weise sämtliche Grössen durch die vorhergehenden bestimmt werden können. So findet man:

$$\begin{aligned} &(1) = p, && (4) = \tfrac{1}{4}(p^4 - p^2), && (7) = \tfrac{1}{7}(p^7 - p)\\ &(2) = \tfrac{1}{2}(p^2 - p), && (5) = \tfrac{1}{5}(p^5 - p), && (8) = \tfrac{1}{8}(p^8 - p^4)\\ &(3) = \tfrac{1}{3}(p^3 - p), && (6) = \tfrac{1}{6}(p^6 - p^3 - p^2 + p), && \text{u. s. w.}\end{aligned}$$

344—346.

Man bemerkt aus diesem Anfang der Reihe, dass das höchste Glied des Ausdrucks (n) gleich $\frac{1}{n}p^n$ ist, zu welchem, wenn n eine Primzahl ist, noch $-\frac{1}{n}p$ hinzutritt; ist aber n eine zusammengesetzte Zahl, so tritt das Gesetz weniger zu Tage. Betrachten wir aber die Sache aufmerksamer, so sehen wir, dass

$$\begin{aligned} p &= (1), & p^5 &= 5(5) + (1)\\ p^2 &= 2(2) + (1) & p^6 &= 6(6) + 3(3) + 2(2) + (1)\\ p^3 &= 3(3) + (1) & p^7 &= 7(7) + (1)\\ p^4 &= 4(4) + 2(2) + (1), & p^8 &= 8(8) + 4(4) + 2(2) + (1) \text{ u. s. w.}\end{aligned}$$

ist, wo das Fortschreitungsgesetz auf der Hand liegt; wenn nämlich $\alpha, \beta, \gamma, \delta, \ldots$ die sämtlichen Teiler von n sind, so ist:

$$p^n = \alpha(\alpha) + \beta(\beta) + \gamma(\gamma) + \delta(\delta) + \cdots$$

Wir gehen nun daran, die Allgemeinheit dieser Bemerkung zu beweisen.

Wir haben gezeigt, dass die Summe aller solcher Ausdrücke $(1^\alpha)(2^\beta)(3^\gamma)\ldots$, falls immer $\alpha + 2\beta + 3\gamma + \cdots = n$ ist, sämtliche Functionen von n Dimensionen erschöpft und daher gleich p^n ist. Hieraus geht hervor, — — —. Wird das Product

$$\left(\frac{1}{1-x}\right)^{(1)}\left(\frac{1}{1-x^2}\right)^{(2)}\left(\frac{1}{1-x^3}\right)^{(3)}\cdots \text{ in die Reihe } 1 + Ax + Bx^2 + \cdots = P$$

entwickelt, so ist:

$$A = p,\quad B = p^2,\quad C = p^3,\ \ldots$$
$$\frac{xdP}{Pdx} = \frac{(1)x}{1-x} + \frac{2(2)x^2}{1-x^2} + \frac{3(3)x^3}{1-x^3}\cdots$$

— — — — — — — —

(hieraus ergiebt sich, wenn man $\frac{px}{1-px}$ für $\frac{xdP}{Pdx}$ substituiert und die einzelnen Brüche in unendliche Reihen entwickelt, die Richtigkeit des Satzes unmittelbar).

347.

Dieser Satz lässt sich auch auf eine andere Weise ausdrücken. Sind nämlich n, 1, δ, δ', δ'', δ''', ... sämtliche Teiler von n, so besteht der Satz darin, dass

$$p^n = n(n) + (1) + \delta(\delta) + \delta'(\delta') + \delta''(\delta'') + \cdots$$

ist.

Nun hat offenbar das Product aus den (n) Primfunctionen, welche von n Dimensionen sind, $n(n)$ Dimensionen und dasselbe gilt von den übrigen, mithin:

Das Product aus allen Primfunctionen von einer Dimension, von n, δ, δ', ... Dimensionen besitzt p^n Dimensionen.

Es ist nun leicht, aus diesem Satze den Wert des Ausdrucks (n) selbst abzuleiten; der Kürze wegen unterdrücken wir aber die Rechnung, welche nicht schwierig ist. Ist daher $n = a^\alpha b^\beta c^\gamma, \ldots$, so dass a, b, c, ... verschiedene Primzahlen sind, so ist:

$$n(n) = p^n - \Sigma p^{\frac{n}{a}} + \Sigma p^{\frac{n}{ab}} - \Sigma p^{\frac{n}{abc}} + \cdots,$$

wo $\Sigma p^{\frac{n}{abc\cdots}}$ den Complex aller Ausdrücke bezeichnet, welche dem Ausdrucke $p^{\frac{n}{abc\cdots}}$ analog sind, wenn man die Grössen a, b, c, ... auf irgend eine Weise unter einander permutiert. So ist z. B. für $n = 36$: $36(36) = p^{36} - p^{18} - p^{12} + p^6$.

Noch eine Bemerkung wollen wir hinzufügen. Ist n von der Form a^α und a prim, so ist $n(n) = p^n - p^{\frac{n}{a}}$; somit wird, da (n) notwendig eine ganze Zahl ist, was auch p sein möge:

$$p^n \equiv p^{\frac{n}{a}} \pmod{n},$$

somit, wenn p prim zu a ist:

$$p^{n-\frac{n}{a}} \equiv 1 \pmod{n},$$

und für $\alpha = 1$:

$$p^{a-1} \equiv 1 \pmod{a}.$$

Es ist bemerkenswert, dass diese Sätze auf so verschiedene Arten gefunden werden können.

348.

Aufgabe. Wenn die Gleichung

$$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} + \cdots + M = 0,$$

deren Wurzeln $x = a$, $x = b$, $x = c$, ... sind, gegeben ist, so soll man eine Gleichung finden, deren Wurzeln $x = a^\tau$, $x = b^\tau$, $x = c^\tau$, ... sind.

Erste Auflösung. Man suche nach dem bekannten Satze die Summe der Wurzeln der gegebenen Gleichung, die Summe ihrer Quadrate, Kuben, u. s. w. bis zur Summe ihrer $m\tau^{\text{ten}}$ Potenzen. Hieraus erhält man daher auch die Summe der Wurzeln der gesuchten Gleichung sowie die Summe ihrer Quadrate u. s. w., nämlich Σa^τ, $\Sigma a^{2\tau}$, ..., woraus demselben Satze zufolge die Coefficienten bestimmt werden können.

Für die Praxis ist diese Lösung zwar die leichtere; für unsern Zweck aber sowie für den Nachweis, dass die Coefficienten der gesuchten Gleichung ganze Zahlen sind, wenn die Coefficienten der gegebenen Gleichung ganze Zahlen sind, ist die folgende zweckmässiger.

Zweite Auflösung. Ist ϑ eine eigentliche Wurzel der Gleichung $x^\tau = 1$ und bildet man das Product aus

$$\begin{array}{llll} x^m + Ax^{m-1} & + Bx^{m-2} & + \cdots \\ x^m + A\vartheta x^{m-1} & + B\vartheta^2 x^{m-2} & + \cdots \\ x^m + A\vartheta^2 x^{m-1} & + B\vartheta^4 x^{m-2} & + \cdots \\ \cdots & \cdots & \cdots \\ x^m + A\vartheta^{\tau-1} x^{m-1} & + B\vartheta^{2\tau-2} x^{m-2} & + \cdots, \end{array}$$

so sind die Wurzeln dieses Products:

$$\begin{array}{lll} a, & \vartheta a, & \vartheta^2 a, \ldots \\ b, & \vartheta b, & \vartheta^2 b, \ldots \\ c, & \vartheta c, & \vartheta^2 c, \ldots \\ & \text{u. s. w.,} & \end{array}$$

d. h. das Product ist dem folgenden gleich:

$$(x^\tau - a^\tau)\,(x^\tau - b^\tau)\,(x^\tau - c^\tau)\cdots$$

und daher von der Form:

$$x^{\tau m} + A' x^{\tau(m-1)} + B' x^{\tau(m-2)} + \cdots$$

Schreibt man nun x für x^τ, so ist:

$$x^m + A' x^{m-1} + B' x^{m-2} + \cdots = (x - a^\tau)\,(x - b^\tau)\,(x - c^\tau) \cdots$$

und daher

$$x^m + A' x^{m-1} + B' x^{m-2} + \cdots = 0$$

die gesuchte Gleichung. Dass aber hier A', B', ... nicht nur rationale, sondern auch ganze Zahlen sind, geht leicht aus der Theorie der Gleichung $x^\tau = 1$ hervor.

Da wir uns dieser Operation im Folgenden oft bedienen werden, so werden wir mit (P, ρ^τ) die Function bezeichnen, welche gleich Null gesetzt eine Gleichung giebt, deren Wurzeln die τ^{ten} Potenzen der Wurzeln der Gleichung $P = 0$ sind.

Ist $P \equiv Q$ nach irgend einem Modul, so ist auch $(P, \rho^\tau) \equiv (Q, \rho^\tau)$ nach demselben Modul.

349.

Satz. Der Coefficient des Gliedes x^n in (P, ρ^τ) ist nach dem Modul τ dem Coefficienten des Gliedes $x^{\tau n}$ in P^τ congruent, wofern τ eine Primzahl ist (was für diesen Fall die dritte Lösung der vorigen Aufgabe ist).

Beweis. Aus dem sechsten Capitel folgt, dass irgend ein Coefficient des Products

$$(x^m + A x^{m-1} + \cdots)\,(x^m + A\vartheta x^{m-1} + \cdots) \cdots,$$

nachdem man für ϑ^τ die Einheit gesetzt hat, die folgende Form erhält:

$$E + (1 + \vartheta + \vartheta^2 + \cdots + \vartheta^{\tau-1}) F.$$

Wenn nun ϑ als eigentliche Wurzel der Gleichung $x^\tau = 1$ betrachtet wird, so geht das ganze Product in E über; setzt man aber $\vartheta = 1$, so geht das ganze Product in $P^\tau = E + \tau F$ über, daher ist der Coefficient des Gliedes $x^{n\tau}$ in P^τ nach dem Modul τ dem Coefficienten des Gliedes $x^{n\tau}$ in E d. h. dem Coefficienten des Gliedes x^n in (P, ρ^τ) congruent.

350.

Satz. Ist τ eine Primzahl, so ist

$$(P, \rho^\tau) \equiv P \pmod{\tau}.$$

Beweis. Es sei der Coefficient des Gliedes x^n in (P, ρ^τ) gleich N', in P aber der Coefficient desselben Gliedes gleich N. Setzt man dann:

$$P = x^m + A x^{m-1} + \cdots + N x^n + \cdots,$$

so ist:

$$P^\tau \equiv x^{m\tau} + A^\tau x^{(m-1)\tau} + \cdots + N^\tau x^{n\tau} + \cdots \text{ (mod. } \tau),$$

und daher (nach vorigem Artikel) $N' \equiv N^\tau$ (mod. τ); mithin wird, da $N^\tau \equiv N$ ist, $N' \equiv N$ sein, w. z. b. w.

Hieraus ist offenbar: $(P, \rho^\alpha) \equiv (P, \rho^{\alpha\tau})$ und $(P, \rho^\tau) \equiv (P, \rho^{\tau^2})$, daher allgemein:

$$(P, \rho^\alpha) \equiv (P, \rho^{\alpha\tau^k}) \text{ (mod. } \tau).$$

351.

Satz. Es giebt einen Wert der Zahl $\nu < p^m$ von der Art, dass die Function $x^\nu - 1$ durch die gegebene Function P von m Dimensionen, deren niedrigstes Glied die Potenz x nicht enthält, nach dem Modul p teilbar ist.

Beweis. Man teile durch P die Reihe der Functionen $1, x, x^2, \ldots, x^{p^m-1}$, sobald dieselben von höherer Dimension als m geworden sind; und da sich keine durch P ohne Rest teilen lässt, so lassen sich sämtliche Reste auf folgende Form bringen:

$$Ax^{m-1} + Bx^{m-2} + \cdots + N,$$

derart, dass sämtliche Coefficienten positiv und kleiner als p sind. Es ist aber klar, dass es, da niemals alle gleich 0 sein können, nur $p^m - 1$ Functionen giebt, deren irgend einer die einzelnen gleich sein müssen; mithin müssen, da man bis zu der Potenz von x, deren Exponent $p^m - 1$ ist, p^m Reste erhält, notwendig wenigstens zwei einander gleich sein. Es möge also derselbe Rest sich ergeben bei der Division von x^a und $x^{a+\nu}$ durch P, so dass $a + \nu < p^m$ ist. Daher lässt sich $x^{a+\nu} - x^a$ durch P teilen. Hiernach kann auch, da (nach Voraussetzung) x und daher auch x^a eine zu P prime Function ist, $x^\nu - 1$ durch P geteilt werden.

Zusatz. Ist $x^\nu - 1$ durch P teilbar, so lässt sich auch $x^{k\nu} - 1$ durch P teilen, wenn k irgend eine ganze Zahl bezeichnet.

352.

Satz. Bleiben die Bezeichnungen wie im vorigen Artikel und ist P eine Primfunction und x^ν die niedrigste Potenz, welche um die Einheit vermindert durch P sich teilen lässt, so ist ν entweder gleich $p^m - 1$ oder ein aliquoter Teil dieser Zahl, den einzigen Fall ausgenommen, wo $P \equiv x$ ist.

Beweis. Da P eine Primfunction von m Dimensionen ist, so giebt es $p^m - 1$ verschiedene Functionen von weniger als m Dimensionen (wenn nämlich von der Anzahl aller die Function 0 ausgeschlossen wird), welche sämtlich prim zu P sind. Da nun x^ν der Annahme nach die niedrigste Potenz ist, welche, durch P geteilt, die Einheit als Rest lässt, so ist klar,

dass, wenn alle niedrigeren Potenzen von 1, x, ... an bis zu $x^\nu - 1$ durch P geteilt werden, ν verschiedene Reste hervorgehen, welche allgemein mit A bezeichnet werden mögen. Wenn nun diese alle Reste, welche möglich sind, erschöpfen, so wird der Satz bewiesen sein; wenn es aber noch einige, nicht unter ihnen befindliche giebt, so sei irgend einer von diesen B. Dann ist ersichtlich, dass die Function Bx^ν durch P geteilt den Rest B giebt und allgemein $Bx^{\nu+k} \equiv Bx^k$ (mod. P) ist. Es geben aber sämtliche Functionen von B an bis zu $Bx^{\nu-1}$ unter sich und von den Resten A verschiedene Reste; denn wenn $Bx^\lambda \equiv Bx^{\lambda+\delta}$ (mod. P) wäre, so würde auch $1 \equiv x^\delta$ (mod. P) und $\delta < \nu$ sein, im Widerspruch mit der Voraussetzung; wenn aber $Bx^\lambda \equiv x^\mu$ (mod. P) wäre, so würde $B \equiv x^{\mu+\nu-\lambda}$ (mod. P) und daher B einer von den Resten A sein, im Widerspruch mit unsrer Annahme. Man erhält daher offenbar noch ν neue Reste. Auf diese Weise kann man weiter fortgehen (ganz so wie oben Artikel ...), und es ist klar, dass die Anzahl aller möglichen $p^m - 1$ Reste entweder $= \nu$ oder $= 2\nu$ oder $= 3\nu$ oder allgemein ein Vielfaches der Zahl ν ist.

353.

Aus dem vorigen Satze und dem Zusatz zu Artikel 351 folgt, dass jede Primfunction von n Dimensionen in der Function $x^{p^n-1} - 1$ nach dem Modul p aufgeht. Demnach werden alle Functionen einer Dimension mit alleiniger Ausnahme derjenigen, welche $\equiv x$ ist, in $x^{p-1} - 1$ aufgehen, und dies ist der Fermat'sche Satz; alle Primfunctionen zweiten Grades aber d. h. diejenigen von der Form $x^2 + Ax + B$ werden in der Function $x^{p^2-1} - 1$ aufgehen u. s. w. Sind nun n, δ, δ', δ'', ..., 1 sämtliche Teiler der Zahl n, so wird offenbar $p^n - 1$ auch durch $p^\delta - 1$, $p^{\delta'} - 1$, $p^{\delta''} - 1$, ..., $p - 1$ teilbar sein; daher lässt sich die Function $x^{p^n-1} - 1$ durch sämtliche Primfactoren von den Dimensionen n, δ, δ', δ'', ... bis zu den Primfunctionen einer Dimension (mit Ausschluss der Function x) und somit (da alle diese Fnnctionen absolut und daher auch unter einander prim sind) auch durch das Product aus allen teilen. Aber eben dieses Product hat $p^n - 1$ Dimensionen (Artikel 347, da die eine Function x darin fehlt), somit ergiebt sich, dass dieses Product der Function $x^{p^n-1} - 1$ nach dem Modul p congruent sein muss.

354.

Satz. Wenn die Function $x^\nu - 1$ durch die Function P teilbar ist, so ist:

$$(P, \rho^{k\nu+t}) \equiv (P, \rho^t),$$

wo k, t beliebige ganze Zahlen vorstellen.

Beweis. Ist

$$P = x^m + Ax^{m-1} + Bx^{m-2} + \cdots,$$

so ist bekanntlich, wenn

$$\frac{mx^{m-1} + (m-1)Ax^{m-2} + \cdots}{x^m + Ax^{m-1} + \cdots}$$

in eine unendliche Reihe von der Form

$$m\frac{1}{x} + \alpha\frac{1}{x^2} + \beta\frac{1}{x^3} + \gamma\frac{1}{x^4} + \cdots$$

entwickelt wird, α die Summe der Wurzeln der Gleichung $P = 0$, β die Summe ihrer Quadrate u. s. w. Hieraus leitet man ohne Mühe her, dass die Summe der $\nu + 1^{\text{ten}}$, $\nu + 2^{\text{ten}}$, ... Potenzen der Summe der Wurzeln, der Summe ihrer Quadrate, u. s. w. respective congruent ist. Hieraus aber folgt, wofern nicht der Modul gleich oder kleiner ist als die Anzahl der Dimensionen der Function P, dass

$$(P, \rho^{\nu+1}) \equiv P,\ (P, \rho^{\nu+2}) \equiv (P, \rho^2),\ (P, \rho^{\nu+3}) \equiv (P, \rho^3), \ldots.$$

ist. Jenen Fall aber werden wir weiter unten betrachten.

355.

Satz. Wenn in der Reihe

$$(P, \rho^0),\ (P, \rho^1),\ (P, \rho^2),\ (P, \rho^3),\ \ldots.$$

die auf das ν^{te} Glied folgenden Glieder den ersten der Reihe nach congruent sind, so wird $x^\nu - 1$ durch P teilbar sein, wofern P keinen Factor mehrere Male enthält.

Beweis. Setzt man $\frac{dP}{dx} = Q$, so wird die Function Q zu P prim sein. Ist

$$\frac{Q}{P} \equiv \frac{A}{x} + \frac{B}{x^2} + \frac{C}{x^3} + \cdots,$$

so wird auf das Glied $\frac{N}{x^\nu}$ (nach Voraussetzung) folgen:

$$\frac{A}{x^{\nu+1}} + \frac{B}{x^{\nu+2}} + \frac{C}{x^{\nu+3}} + \cdots$$

Daher ist:

$$\frac{Q}{P} \equiv \frac{Ax^{\nu-1} + Bx^{\nu-2} + \cdots}{x^\nu - 1},$$

woraus hervorgeht, dass die Function $x^\nu - 1$ durch P geteilt werden kann.

356.

Satz. Wenn P eine Primfunction von x von m Dimensionen und X eine Function von $x, x^p, x^{p^2}, x^{p^3}, \ldots, x^{p^{m-1}}$ ist, in welche alle diese Grössen in gleicher Weise eingehen, d. h. welche die-

selbe bleibt, auf welche Weise diese Grössen auch unter einander vertauscht werden mögen, so giebt die Function X durch P geteilt einen Rest, welcher eine Zahl ist.

Beweis. Ist der Rest

$$Ax^{m-1} + Bx^{m-2} + \cdots + N \equiv \xi,$$

so werden alle Coefficienten A, B, C, ... bis zu N, diesen ausgeschlossen, $\equiv 0$ sein. Dies wird folgendermassen bewiesen. Da $X - \xi$ durch P teilbar ist, so lässt sich auch $X^p - \xi^p$ durch P teilen. Man sieht aber leicht, dass X^p das ist, was aus X wird, wenn man x^p für x, x^{p^2} für x^2, u. s. w. und x^{p^m} oder, was dasselbe ist, x für $x^{p^{m-1}}$ setzt. Hiernach ist offenbar $X^p \equiv X$ (mod. P); somit wird, da $X^p \equiv \xi^p$ und $X \equiv \xi$ (mod. P) ist, auch $\xi^p \equiv \xi$ (mod. P) oder

$$\xi^p - \xi \equiv 0 \text{ (mod. } P)$$

sein. Es ist aber $\xi^p - \xi$ nach dem Modul p congruent dem Producte aus ξ, $\xi + 1$, $\xi + 2$, ... bis zu $\xi + p - 1$, welche Factoren sämtlich prim zu P sein werden, wenn nicht ξ einfach eine Zahl ist. Daher kann auch $\xi^p - \xi$ in keiner andern Weise durch P teilbar sein.

Derartige Functionen sind die Summe aller jener Grössen, die Summe ihrer Quadrate, Kuben, u. s. w., die Summe der Producte aus je zweien, dreien u. s. w. Welches aber jene Zahl sei, werden wir im folgenden Artikel bestimmen.

357.

Satz. Ist die Primfunction des vorigen Artikels

$$P \equiv x^m - Ax^{m-1} + Bx^{m-2} - Cx^{m-3} + \cdots,$$

so ist der Rest, wenn die Summe der Grössen x, x^p, ..., $x^{p^{m-1}}$ durch P dividiert wird, $\equiv A$, wenn die Summe der Producte aus je zweien durch P dividiert wird, $\equiv B$, wenn die Summe der Producte aus je dreien dividiert wird, $\equiv C$, u. s. w.

Beweis. Es seien jene Functionen X, Y, Z, ... und ihre Reste in ihrer Reihenfolge A', B', C', ... Dann sieht man leicht, dass x, x^p, x^{p^2}, ... die Wurzeln der Gleichung

$$z^m - Xz^{m-1} + Yz^{m-2} - Zz^{m-3} + \cdots = 0$$

sind. Setzt man daher $z = x$, so wird:

$$x^m - Xx^{m-1} + Yx^{m-2} - Zx^{m-3} + \cdots$$

Die Functionen $X - A'$, $Y - B'$, $Z - C'$, ... lassen sich aber durch P teilen, daher auch die Function

$$x^m - A'x^{m-1} + B'x^{m-2} - C'x^{m-3} + \cdots$$

Dies kann aber nicht anders der Fall sein, als wenn $A' \equiv A$, $B' \equiv B$, $C' \equiv C$, ... ist.

Übrigens ist bekannt, dass, welche andere Function X von x, x^p, x^{p^2}, ... (in die alle diese Grössen in gleicher Weise eingehen) auch sein möge, dieselbe immer aus diesen abgeleitet werden kann. So ist z. B.

$$x^2 + x^{2p} + x^{2p^2} + \cdots \equiv A^2 - 2B \text{ (mod. } P) \text{ u. s. w.}$$

Beispiel. Ist $p = 5$ und $P \equiv x^2 + 2x + 3$, so ist die Function $x + x^5$, durch P geteilt, $\equiv -2$, $x^6 \equiv 3$ u. s. w.

358. 359.

Satz. Ist P eine Primfunction und x^ν die niedrigste Potenz von x, welche durch P dividiert den Rest 1 giebt, ist ferner $P \equiv (P, \rho^n)$, so wird n irgend einer Potenz der Zahl p nach ν congruent sein.

Beweis. Oben haben wir gezeigt, dass, wenn

$$P = x^m + Ax^{m-1} + Bx^{m-2} + \cdots$$

ist, alsdann

$$z^m + Az^{m-1} + Bz^{m-2} + \cdots - (z-x)(z-x^p)\cdots(z-x^{p^{m-1}})$$

durch P teilbar ist. In ähnlicher Weise würde folgen, dass

$$z^m + Az^{m-1} + Bz^{m-2} + \cdots - (z-x^n)(z-x^{np})\cdots(z-x^{np^{m-1}})$$

durch P teilbar ist. Da nun aber diese Factoren unter einander prim sind, so muss offenbar jeder einzelne jedem einzelnen nach P, p congruent sein. Daher muss notwendig $z - x^n \equiv z - x^{p^\varkappa}$, d. h. $p^\varkappa \equiv n$ (mod. ν) sein. W. z. b. w.*)

---

*) Ist $(P, \rho^a) \equiv (P, \rho^b)$ (mod. p), so ist $a \equiv p^\varkappa b$ (mod. ν).

Beweis. Ist $z^m + Az^{m-1} + Bz^{m-2} + \cdots = \Pi$, so ist $(\Pi, \rho^a) \equiv (\Pi, \rho^b)$ (mod. P). Es ist aber:

$$(\Pi, \rho^a) \equiv (z-x^a)(z-x^{ap})(z-x^{ap^2})\cdots(z-x^{ap^{m-1}}),$$
$$(\Pi, \rho^b) \equiv (z-x^b)(z-x^{bp})(z-x^{bp^2})\cdots(z-x^{bp^{m-1}}),$$

und hieraus ergiebt sich der Satz.

Das Product aus Π, (Π, ρ^2), (Π, ρ^3), ..., (Π, ρ^ν) ist $\equiv (z^\nu - 1)^m$ (mod. P); denn es ist:

$$(z-x)(z-x^2)(z-x^3)\cdots(z-x^\nu) \equiv (z-x^p)(z-x^{2p})(z-x^{3p})\cdots(z-x^{\nu p}) \equiv \cdots \equiv z^\nu - 1.$$

In der Reihe P, (P, ρ^2), (P, ρ^3), ..., (P, ρ^ν) kommen alle Primteiler der Function $x^\nu - 1$ vor und zwar jeder m-mal. Daraus geht hervor, dass das Product aus allen $\equiv (x^\nu - 1)^m$ ist.

Über die Auffindung der Primteiler der Function $x^\nu - 1$ nach einem primen Modul.

360.

Wenn ν durch den Modul p oder durch irgend eine Potenz desselben teilbar und etwa $\nu = p^k\lambda$ ist, so wird

$$x^\nu - 1 \equiv (x^\lambda - 1)^{p^k} \pmod{p}$$

sein. Hieraus geht hervor, dass man nur den Fall zu betrachten braucht, wo ν durch p nicht teilbar ist.

Ist $p^m \equiv 1 \pmod{\nu}$ und zwar m möglichst klein, so wird offenbar $x^{p^m-1} - 1$ durch $x^\nu - 1$ teilbar sein. Daher kann $x^\nu - 1$ keine anderen Factoren haben, als $x^{p^m-1} - 1$. Dieser Ausdruck aber hat prime Teiler von m Dimensionen und andere, bei denen die Anzahl der Dimensionen ein Teiler der Zahl m ist. Solche Teiler wird also auch $x^\nu - 1$ haben. Wie viele von jeder Art aber diese Function hat, wollen wir durch ein Beispiel klarlegen, woraus leicht das allgemeine Gesetz abgeleitet werden kann.

Ist $\nu = 63$ und $p = 13$, so ist $m = 6$. Daher wird $x^{63} - 1$ nach dem Modul 13 Primfactoren haben von sechs, drei, zwei und einer Dimension. Nun ist klar, dass das Product aus den Factoren einer Dimension der gemeinschaftliche Teiler (von höchster Dimension) der Functionen $x^{63} - 1$ und $x^{12} - 1$ d. i. $x^3 - 1$ ist. Daher giebt es drei Primfactoren von einer Dimension. Das Product aus allen Primfactoren von zwei Dimensionen und von einer wird gemeinschaftlicher Teiler der Functionen $x^{63} - 1$ und $x^{168} - 1$, d. h. $x^{21} - 1$ sein; daher giebt es $\frac{21-3}{2}$ oder 9 Factoren von zwei Dimensionen. Das Product aus den Primfactoren von drei Dimensionen und von einer Dimension wird gemeinschaftlicher Teiler der Functionen $x^{63} - 1$ und $x^{2196} - 1$ d. h. $x^9 - 1$ sein; daher giebt es $\frac{9-3}{3} = 2$ Teiler von drei Dimensionen. Die übrigen endlich sind von sechs Dimensionen und ihre Anzahl sonach gleich $\frac{63-6-18-3}{6}$ d. h. gleich 6.

Durch aufmerksame Erwägung dieses Gegenstandes erhält man leicht die folgende allgemeine **Regel**:

Es sei δ ein Teiler von m, und es seien $\delta', \delta'', \delta''', \ldots$ sämtliche Teiler der Zahl δ, welche kleiner als δ sind. Ferner seien die grössten gemeinschaftlichen Teiler zwischen ν und $p^\delta - 1$, $p^{\delta'} - 1$, $p^{\delta''} - 1, \ldots$ respective $\mu, \mu', \mu'', \ldots$ und $\frac{\mu}{\mu'}, \frac{\mu}{\mu''}, \frac{\mu}{\mu'''}, \cdots$ respective $= \lambda', \lambda'', \lambda''', \ldots$. Dann hat $x^\nu - 1$ $\frac{1}{\delta}$-mal soviel Primteiler von

δ Dimensionen, als es unterhalb der Zahl μ Zahlen giebt, die durch keine der Zahlen $\lambda', \lambda'', \lambda''', \ldots$ teilbar sind.

361.

Satz. Wenn die Function X der unbestimmten Grösse x durch eine andere ξ sich teilen lässt und X, wenn x^k für x geschrieben wird, in X' übergeht, so lässt sich X' durch $(\xi, \rho^{\frac{1}{k}})$ teilen.

Beweis. Ist $X \equiv \xi v$ und gehen ξ, v in ξ', v' über, wenn x^k für x geschrieben wird, so ist offenbar $X' \equiv \xi' v'$. Aber ξ' lässt sich durch $(\xi, \rho^{\frac{1}{k}})$ teilen. Mithin auch X'.

362.

Nach Feststellung dieser Prinzipien können wir nun leicht die Primteiler der Function $x^\nu - 1$ bestimmen. Wir nehmen an, dass alle diejenigen, welche auch irgend eine Function $x^{\nu'} - 1$, wo $\nu' < \nu$ ist, teilen, schon gefunden seien, und dass es sich darum handelt, die übrigen zu ermitteln. Diese lassen sich aber sämtlich in dem Ausdrucke (P, ρ^k) zusammenfassen, wenn P eine von ihnen ist und für k alle Zahlen substituiert werden, welche kleiner als ν und prim zu ν sind.

Im sechsten Kapitel haben wir gezeigt, auf welche Weise die eigentlichen Wurzeln der Gleichung $x^\nu = 1$ so in Klassen geteilt werden können, dass man, nachdem alle durch Potenzen irgend einer von ihnen ausgedrückt sind, dieselbe Verteilung in die einzelnen Klassen erhält, welche eigentliche Wurzel man auch als diese Basis nehmen möge. Derartige Complexe der Wurzeln werden wir Perioden nennen. Es ist nun klar, dass die Functionen $x, x^\alpha, x^\beta, x^\gamma, \ldots$, wo $\alpha, \beta, \gamma, \ldots$ sämtliche zu ν primen Zahlen bezeichnen, in ähnlicher Weise in Perioden zerlegt werden können und jede grössere Periode wiederum in kleinere, bis man endlich zu Perioden von der Form $x^k, x^{kp}, x^{kp^2}, \ldots, x^{kp^{m-1}}$ gelangt. Ist dies geschehen, so wird offenbar

1. da jede Periode aus derartigen kleinsten Perioden $x^k + x^{kp} + \cdots$ zusammengesetzt ist, der Rest eine blosse Zahl sein, wenn man sie durch irgend eine Primfunction von m Dimensionen dividiert.

2. Da stets alle Glieder einer Periode auf die Form $x^{\varkappa \cdot a^\alpha b^\beta c^\gamma \cdots}$ gebracht werden können, wo $\varkappa, a, b, c \ldots$ bestimmte Zahlen sind, für $\alpha, \beta, \gamma, \ldots$ aber alle Werte substituiert werden können, so ist klar, dass die Periode in sich selbst übergeht, wenn x^k für x gesetzt wird und k von der Form $a^\alpha b^\beta c^\gamma \ldots \pmod{\nu}$ ist, woraus leicht ersichtlich ist, dass alle Functionen $P, (P, \rho^k), \ldots$, wenn k eine solche Zahl bezeichnet, bei der Division der Periode durch sie denselben Rest hervorbringen.

3. Mithin lässt sich die Periode, nachdem man einen solchen Rest subtrahiert hat, durch das Product aus allen Functionen (P, ρ^k) teilen.

363.

Es handelt sich also hauptsächlich darum, diese Reste zu bestimmen. Zunächst suche man den Rest, welchen die grösste Periode bei der Division durch das Product aus allen hergehörigen Primfunctionen übriglässt. Ist dieses Product

$$\equiv x^\lambda - Ax^{\lambda-1} + \cdots,$$

so ist dieser Rest $\equiv A$. Die Form dieses Products findet man aber leicht, und aus dem sechsten Kapitel ergiebt sich, dass $A = 0$ ist, wenn ν durch ein Quadrat teilbar ist, dass dagegen A entweder $= +1$ oder $= -1$ ist, je nachdem die Anzahl der Primfactoren der Zahl ν gerade oder ungerade ist.

Man löse nun diese grösste Periode in kleinere Perioden auf und stelle die Perioden jeden Gliedes durch $x^{kp^\pi u}$ dar, so dass k in jeder Periode eine bestimmte, für verschiedene Perioden aber veränderliche Zahl ist, π und u aber in jeder Periode veränderliche Zahlen sind, jedoch diejenigen Werte, welche sie in irgend einer Periode haben, auch in den übrigen erhalten können. Nimmt man für den Augenblick irgend eine Primfunction P als Basis und ist der Rest, welchen die Perioden $\Sigma x^{p^\pi u}$, $\Sigma x^{k'p^\pi u}$, ..., durch P geteilt, übriglassen, respective A, A', ..., so wird $\Sigma x^{p^\pi u} - A$ durch das Product aus allen Functionen (P, ρ^u), $\Sigma x^{k'p^\pi u} - A'$ durch das Product aus allen Functionen $(P, \rho^{k'u})$ u. s. w. teilbar sein. Es ist aber leicht ersichtlich, dass die Grössen A, A', ... Wurzeln der gegebenen Congruenz sind. Sind nämlich die Perioden der Wurzeln der Gleichung $x^\nu = 1$, welche den vorigen Perioden entsprechen, Wurzeln der Gleichung $Q = 0$, so werden A, A', ... Wurzeln der Congruenz $Q \equiv 0$ sein. Denn es ist:

$$A + A' + \cdots \equiv \text{der Summe der Perioden,}$$
$$A^2 + A'^2 + \cdots \equiv \text{der Summe der Quadrate der Perioden,}$$
u. s. w.

Die Rechnung ist nämlich derjenigen völlig analog, welche wir im sechsten Kapitel auseinandergesetzt haben, falls man x für ρ setzt, da auch hier für x^ν die Einheit gesetzt werden kann, wie dort für ρ^ν.

Hat man die Wurzeln A, A', ... gefunden, so wähle man irgend eine als Rest der Periode $\Sigma x^{p^\pi u}$ aus und ordne danach die Reste der übrigen in ähnlicher Weise wie im sechsten Kapitel. Denn jene Wahl wird auch hier willkürlich gelassen, da die Function P bisher völlig unbestimmt ist. Die folgende Rechnung ist durchaus derjenigen analog, welche wir im sechsten Kapitel ausführlich behandelt haben; die Einzelheiten hier auseinanderzusetzen, würde uns viel zu weit führen. Nachdem man schliesslich zu Σx^{p^π} gelangt ist, ist die ganze Sache abgemacht. Denn setzt man:

$$P \equiv x^m + ax^{m-1} + bx^{m-2} + \cdots,$$

so ist $-a \equiv \Sigma x^{p^\pi}$; in derselben Weise erhält man den zweiten Coefficienten

der übrigen Functionen (P, ρ^k), woraus die andern Coefficienten von P bestimmt werden können. Öfters kann der Fall eintreten, dass man zu identischen Congruenzen gelangt, aus denen dem Anschein nach nichts gefolgert werden kann. Wie man dieser Schwierigkeit begegnen kann, werden wir weiter unten zeigen.

364.

Alles dies wird durch ein **Beispiel** viel klarer werden. Es sei die Aufgabe gestellt, die Function $x^{15} - 1$ nach dem Modul 17 in Factoren zu zerlegen. Hier ist $m = 5$, und da das Product aus allen elementaren Functionen

$$\equiv \frac{(x^{15}-1)(x-1)}{(x^3-1)(x^5-1)} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

ist, so giebt es nur zwei Primfactoren von vier Dimensionen P und P'. Nun zerlege man $x, x^2, x^4, x^7, x^8, x^{11}, x^{13}, x^{14}$ in die folgenden beiden Perioden:

$$\Sigma x^{17^\alpha} \equiv x + x^2 + x^4 + x^8,$$
$$\Sigma x^{7\cdot 17^\alpha} \equiv x^7 + x^{11} + x^{13} + x^{14}.$$

Ist nach einer der beiden Functionen P, P':

$$\Sigma x^{17^\alpha} \equiv A, \quad \Sigma x^{7\cdot 17^\alpha} \equiv A',$$

so ist:

$$A + A' \equiv 1$$
$$A^2 \equiv \Sigma x^{2\cdot 17^\alpha} + \Sigma x^{3\cdot 17^\alpha} + \Sigma x^{5\cdot 17^\alpha} + \Sigma x^{9\cdot 17^\alpha}$$
$$A'^2 \equiv \Sigma x^{14\cdot 17^\alpha} + \Sigma x^{6\cdot 17^\alpha} + \Sigma x^{5\cdot 17^\alpha} + \Sigma x^{3\cdot 17^\alpha},$$

mithin:

$$A^2 + A'^2 \equiv \Sigma x^{17^\alpha} + \Sigma x^{7\cdot 17^\alpha} + 4\Sigma x^{3\cdot 17^\alpha} + 2\Sigma x^{5\cdot 17^\alpha} \equiv 1 - 4 - 4 \equiv -7.$$

Hiernach sind A, A' die Wurzeln der Congruenz:

$$x^2 - x + 4 \equiv 0 \pmod{17}$$

und diese sind 6, 12. Somit wird P ein Teiler sein von

$$x^8 + x^4 + x^2 + x - 6,$$

und zwar ist derselbe:

$$\equiv x^4 - 6x^3 - 2x^2 - 12x + 1,$$

P' aber wird $\equiv (P, \rho^7)$ und daher

$$\equiv x^4 - 12x^3 - 2x^2 + 6x + 1$$

sein.

365.

Es genügt uns hier, die Möglichkeit dieser Lösungen gezeigt zu haben. Die vielen Kunstgriffe, durch welche diese Rechnungen erleichtert werden können, übergehen wir der Kürze wegen. Dagegen können wir einige sehr wichtige Folgerungen nicht unerwähnt lassen.

Durch das Vorhergehende ist bewiesen worden, dass alle Hülfsgleichungen für die Auflösung der Gleichung $x^\nu = 1$, wenn sie in Congruenzen verwandelt werden, mögliche Wurzeln haben, sobald die Periode

$$x + x^p + x^{p^2} + \cdots + x^{p^{m-1}}$$

noch nicht zerlegt ist. Nehmen wir den Fall, wo ν eine Primzahl ist, so ist m ein Teiler von $\nu - 1$. Hier werden also die Hülfsgleichungen, wenn die Anzahl der Perioden, welche durch jene gefunden werden, ein aliquoter Teil der Zahl $\frac{\nu-1}{m}$ ist, reelle Wurzeln haben. Wenn daher $\frac{\nu-1}{m}$ gerade ist, d. h. wenn m ein Teiler der Zahl $\frac{\nu-1}{2}$ oder wenn $p^{\frac{\nu-1}{2}} \equiv 1 \pmod{\nu}$ oder wenn p quadratischer Rest der Primzahl ν ist, so wird die quadratische Gleichung, durch welche die Wurzeln in zwei Perioden geteilt werden, reelle Wurzeln nach dem Modul p besitzen. Im sechsten Kapitel haben wir aber gezeigt, dass diese Gleichung, wenn man $\nu = 4n \pm 1$ setzt, stets $x^2 + x \mp n = 0$ ist. Mithin erhalten wir folgenden bemerkenswerten

Satz. Wenn die Primzahl p quadratischer Rest der Primzahl $4n \pm 1$ ist, so wird die Congruenz

$$x^2 + x \mp n \equiv 0 \pmod{p}$$

und daher auch die Congruenz

$$4x^2 + 4x \mp 4n \equiv 0 \text{ oder } (2x+1)^2 \mp \nu \equiv 0$$

reelle Wurzeln haben, d. h. es wird $\pm \nu$ quadratischer Rest der Zahl p sein.

366.

Dies ist also der dritte vollständige Beweis des Fundamentaltheorems im vierten Kapitel, der um so mehr beachtenswert ist, weil die Prinzipien, aus denen er abgeleitet ist, von denen, deren wir uns zu den früheren Beweisen bedient haben, völlig verschieden sind. Aus eben dieser Quelle aber, jedoch auf dem entgegengesetzten Wege, wollen wir einen vierten Beweis ableiten. Ist nämlich ν eine Primzahl von der Fom $4n \pm 1$, p eine beliebige andere Primzahl, und ist $\pm \nu$ quadratischer Rest der Primzahl p, so werden wir beweisen, dass p quadratischer Rest der Zahl ν ist.

Es sei p^m die kleinste Potenz der Zahl p, welche $\equiv 1 \pmod{\nu}$ ist. Die Elementarteiler der Function $\frac{x^\nu - 1}{x - 1}$ nach p werden m Dimensionen haben,

daher die Anzahl aller gleich $\frac{\nu-1}{m}$ ist. Da nun $\pm\,\nu Rp$ ist, so ist die Congruenz

$$x^2 + x \mp n \equiv 0 \pmod{p}$$

auflösbar; ihre Wurzeln seien A und A'. Verteilt man die Functionen $x, x^2, \ldots, x^{\nu-1}$ in zwei Klassen, welche mit ξ und ξ' bezeichnet werden mögen, so ist:

$$\xi + \xi' \equiv A + A' + (1 + x + x^2 + \cdots + x^{\nu-1})$$
$$\xi\xi' \equiv AA' + \lambda(1 + x + x^2 + \cdots + x^{\nu-1}),$$

somit wird

$$(z-\xi)(z-\xi') - (z-A)(z-A')$$

durch jeden Elementarteiler der Function $\frac{x^\nu - 1}{x-1}$ teilbar sein. Hiernach aber wird jeder dieser Elementarteiler entweder in $\xi - A$ und $\xi' - A'$ oder in $\xi - A'$ und $\xi' - A$ aufgehen. Hieraus geht hervor (da A nicht $\equiv A'$ ist), dass, wenn man x^p für x setzt, ξ und ξ' nicht geändert werden. Denn wenn ξ in ξ' und umgekehrt überginge, so würden $\xi - A$ und $\xi - A'$ durch dieselbe Primfunction teilbar sein, was absurd ist. Hieraus folgt endlich, dass $\frac{\nu-1}{2}$ durch m oder $p^{\frac{\nu-1}{2}} - 1$ durch ν teilbar ist. Demnach ist p quadratischer Rest von ν.

Es ist aber leicht, alle Fälle des Fundamentaltheorems aus jedem der beiden Sätze abzuleiten.

367.

Obwohl wir uns hier auf den Fall, wo ν eine Primzahl ist, beschränkt haben, können doch auch, wenn ν eine zusammengesetzte Zahl ist, analoge Sätze ohne grosse Mühe aufgestellt werden, was wir jetzt der Kürze halber nicht ausführlicher auseinandersetzen können.

Es ist klar, dass ähnliche Bemerkungen auch über eine grössere Anzahl von Perioden gemacht werden können. So wird, wenn $\frac{\nu-1}{m}$ durch 3 teilbar ist, d. h. wenn p kubischer Rest der Primzahl ν ist, die Gleichung, vermittelst deren die Wurzeln der Gleichung $x^\nu = 1$ in drei Perioden geteilt werden und die wir im sechsten Kapitel a priori zu bestimmen gelehrt haben, nach dem Modul p auflösbar sein und umgekehrt. So kann z. B. die Congruenz $x^3 + x^2 - 2x - 1 \equiv 0$ nach einem beliebigen Primzahlmodul, welcher von der Form $7n \pm 1$ ist, aufgelöst werden, während dies nicht möglich ist, wenn der Modul eine andere Form besitzt.

Es würde uns nicht schwer fallen, dieses Kapitel noch mit vielen andern Bemerkungen zu bereichern, wenn nicht die Grenzen, auf welche wir uns beschränken müssen, dies verbieten würden. Denjenigen, welche weiter vorgehen möchten, werden diese Prinzipien wenigstens den Weg andeuten können.

368.

Wir sagen, irgend eine Congruenz $S\equiv 0$ habe gleiche Wurzeln oder allgemeiner gleiche Teiler, wenn sie sich durch eine Potenz irgend einer Function teilen lässt.

Ob eine gegebene Congruenz gleiche Teiler habe, lässt sich in derselben Weise entscheiden, wie in der Theorie der Gleichungen. Setzt man

$$X\equiv \xi^m P,$$

so wird offenbar:

$$\frac{dX}{dx}\equiv \xi^{m-1}\left(mP\frac{d\xi}{dx}+\xi\frac{dP}{dx}\right),$$

mithin wird $\frac{dX}{dx}$ durch ξ^{m-1} teilbar sein. Ist allgemein

$$X\equiv A^a B^b C^c \ldots,$$

wo A, B, C, ... verschiedene Primfunctionen bezeichnen, so ist:

$$\frac{dX}{dx}\equiv X\left(\frac{adA}{Adx}+\frac{bdB}{Bdx}+\frac{cdC}{Cdx}+\cdots\right),$$

woraus hervorgeht, dass, wenn nicht eine der Zahlen a, b, c, ... durch den Modul teilbar ist, $\frac{dX}{dx}$ durch $A^{a-1}B^{b-1}C^{c-1}\ldots$, nicht aber durch A^a, B^b, $C^c \ldots$ geteilt werden kann. Hieraus folgt der

Satz. Wenn der gemeinschaftliche Teiler grösster Dimension der beiden Functionen X und $\frac{dX}{dx}$ gleich ξ ist, so wird X alle Primfactoren, welche ξ hat, ebenfalls besitzen, und zwar jeden einmal mehr als ξ; wenn daher X und $\frac{dX}{dx}$ zu einander prime Functionen sind, so wird X keine gleichen Factoren haben.

369.

Erstes Beispiel. Man will wissen, ob die Function

$$x^5+3x^4-6x^3+3x-4=X$$

nach dem Modul 17 gleiche Teiler hat. — Es ist:

$$\frac{dX}{dx}\equiv 5x^4-5x^3-x^2+3.$$

Hieraus findet man, dass die Functionen X und $\frac{dX}{dx}$ prim zu einander sind, weshalb X keine gleichen Factoren hat.

Zweites Beispiel. Ist

$$X \equiv x^5 + 6x^4 - 3x^3 - 4x^2 + 2x - 3 \text{ (mod. 13)},$$

so ist:

$$\frac{dX}{dx} \equiv 5x^4 - 2x^3 + 4x^2 + 5x + 2.$$

Der grösste gemeinschaftliche Teiler der Functionen X und $\frac{dX}{dx}$ aber ist $\equiv 5x^2 + 7x + 7$, oder nach Multiplikation mit $8: \equiv x^2 + 4x + 4$; und da dieser Teiler $\equiv (x+2)^2$ ist, so wird die Function X durch $(x+2)^3$ teilbar sein und der Quotient (welcher gleich $x^2 + 11$ ist) enthält keinen doppelten Teiler weiter.

370. 371.

Wenn nach den vorhergehenden Artikeln die Function X in der Form $A^a B^b C^c \ldots$ dargestellt ist, so dass A, B, C, ... zu einander prime Functionen und die Zahlen a, b, c, ... ungleich sind, so lässt sich die Zerlegung noch weiter ausdehnen. Es sei also X eine Function, welche keine gleichen Teiler weiter enthält. Wir sahen oben, dass $x^p - x$ das Product aus allen Primfunctionen von einer Dimension ist. Ist ξ der gemeinschaftliche Teiler höchster Dimension der beiden Functionen X und $x^p - x$, so wird ξ das Product aus allen Teilern von X von einer Dimension sein und $\frac{X}{\xi}$ wird derartige Teiler nicht mehr besitzen. Wenn man aber findet, dass die Functionen X und $x^p - x$ zu einander prim sind, so wird X keinen Teiler von einer Dimension und daher die Congruenz $X \equiv 0$ keine reellen Wurzeln haben. Da ferner $x^{p^2} - x$ das Product aus allen Primfunctionen von zwei Dimensionen und von einer Dimension ist, so wird der gemeinschaftliche Teiler höchster Dimension von den Functionen $x^{p^2} - x$ und $\frac{X}{\xi}$, etwa ξ', sämtliche Teiler von X enthalten, welche von zwei Dimensionen sind. Geht man so weiter fort, so sieht man hieraus, dass X auf diese Weise in Factoren ξ, ξ', ξ'', ... zerlegt wird, welche respective alle Teiler von einer, von zwei, drei, u. s. w. Dimensionen enthalten.

372.

Wenn aber das Product aus mehreren Primfunctionen von derselben Dimension gegeben ist, so werden die einzelnen Functionen durch Probieren bestimmt werden müssen. Diese Aufgabe hat grosse Ähnlichkeit mit derjenigen, wonach die Factoren zusammengesetzter Zahlen gesucht werden sollen. Hier ist aber schon a priori bestimmt, ob eine gegebene Function noch in Factoren zerlegt werden kann. Da auch hier die Anzahl aller möglichen Factoren eine endliche ist, so können wir uns eines ähnlichen Hülfsmittels wie oben bedienen. Doch wollen wir uns mit diesem Gegenstande nicht aufhalten, da ein geübter Rechner, der die Prin-

zipien wohl beherrscht, leicht, wenn es nötig sein sollte, besondere Kunstgriffe finden wird.

Wir gehen zu einem andern Kapitel über, nämlich zur Betrachtung von Congruenzen, wenn der Modul nicht eine Primzahl ist, wie wir bisher immer angenommen haben. Besonders aber ist hier jener Fall sowohl an und für sich als auch deshalb der Beachtung wert, wo der Modul eine Potenz einer Primzahl ist, weil er zur Beseitigung einiger Zweifel (Artikel ...) notwendig ist.

373.

Aufgabe. Wenn die Function X nach dem Modul p in zu einander prime Factoren $\xi, \xi', \xi'', \ldots$ zerlegt ist, so soll man X nach dem Modul p^2 in ähnliche Factoren $\Xi, \Xi', \Xi'', \ldots$ so zerlegen, dass

$$\xi \equiv \Xi,\ \xi' \equiv \Xi',\ \xi'' \equiv \Xi'', \ldots \pmod{p}$$

ist.

Auflösung. Ist $X \equiv \xi\psi \pmod{p}$ oder $X = \xi\psi + p\Sigma$ und setzt man:

$$\Xi = \xi + p\varphi,\ \Psi = \psi + p\omega,$$

so wird

$$\Xi\Psi = X - p\Sigma + (\varphi\psi + \xi\omega)p + p^2\varphi\omega$$

sein. Wenn also $\Xi\Psi \equiv X \pmod{p^2}$ sein soll, so muss notwendig $\varphi\psi + \xi\omega - \Sigma$ durch p teilbar sein. Da aber ψ und ξ nach dem Modul p zu einander prime Functionen sind, so können φ und ω so bestimmt werden, dass diese Bedingung erfüllt ist (Artikel 336), und zwar überdies so, dass die Dimensionen von φ und ω um eine Einheit niedriger sind, als die Dimensionen der Functionen ξ, ψ respective. Hiernach wird $X \equiv \Xi\Psi \pmod{p^2}$. Es ist klar, dass auf ähnliche Weise Ψ wiederum in Factoren $\Xi'\Omega$ zerlegt werden kann, so dass die eine $\Xi' \equiv \xi' \pmod{p}$ ist, u. s. w., wodurch man schliesslich erhält:

$$X \equiv \Xi\Xi'\Xi'' \ldots \pmod{p^2}.$$

374.

Hiernach lässt sich leicht beweisen, dass X auch nach den Moduln $p^3, p^4, \ldots$ in Factoren zerlegt werden kann. Ist allgemein

$$X \equiv PQ \pmod{p^m} \text{ oder } X = PQ + p^m R$$

und ist die Function P zu Q nach dem Modul p prim, setzt man ferner:

$$P' = P + Ap^m,\ Q' = Q + Bp^m,$$

so wird:

$$P'Q' = X - p^m R + (AQ + BP)p^m + ABp^{2m}.$$

Hieraus ist für jeden Modul p^ν (wo $\nu > m$ und $< 2m+1$ ist):

$$P'Q' \equiv X, \text{ wenn } R \equiv AQ + BP \pmod{p^{\nu - m}} \text{ ist.}$$

40*

Aus diesem ersieht man, dass, wenn die Function X nach dem Modul p keine gleichen Factoren hat, dieselbe nach dem Modul p^k in ähnlicher Weise in Factoren zerlegt werden kann, wie nach dem Modul p. Wenn aber X gleiche Factoren hat, so wird die Sache bei weitem complicierter und lässt sich sogar mittelst der vorhergehenden Prinzipien nicht vollständig erledigen. Daher wollen wir, da wir nicht Alles, was hierher gehört, mitteilen können, nur einen einzigen Fall betrachten, welcher am häufigsten vorkommt und dessen Entwicklung zur Lösung einiger im Vorhergehenden übriggebliebener Zweifel erforderlich ist. Dieser Fall ist der, wo nur gleiche Factoren von einer Dimension in Betracht kommen. Dieser kann in zweckmässiger Weise auch zur Auffindung der Wurzeln der Congruenzen benutzt werden. Bei anderer Gelegenheit werden wir diesen Gegenstand allgemein behandeln.

375.

Es sei also $X \equiv X'(x-a)^m \pmod{p}$ und die Function X' prim zu $x-a$; gesucht werden alle Teiler von X von einer Dimension, welche dem Teiler $x-a$ nach dem Modul p, X selbst aber nach den Moduln p^2, p^3, ... congruent sind. (Wir setzen voraus, dass die Function X absolut durch $x-a$ nicht geteilt werden kann, denn sonst würde $x-a$ die Function X nach jedem beliebigen Modul teilen.) Substituiert man $z+a$ für x, so erhält man:

$$Z \equiv Z'z^m \pmod{p} \quad \text{oder} \quad Z = Z'z^m + pA.$$

Wenn nun Z nach dem Modul p^2 durch irgend einen Teiler von der Form $z+\alpha p$ geteilt werden kann, so muss A notwendig von der Form $zZ''+pB$ sein. Ist dieses nicht der Fall, so ist die Untersuchung bereits beendet. Setzen wir also:

$$Z \equiv Z'z^m + pZ''z \pmod{p^2}, \quad \text{oder}$$
$$Z = Z'z^m + pZ''z + p^2B,$$

so ist klar, dass Z durch z und jeden andern diesem nach dem Modul p congruenten Teiler geteilt werden kann.

Um einen bestimmten Fall vor uns zu haben, setzen wir $m=4$; es ist leicht ersichtlich, dass jeder andere Fall in analoger Weise behandelt werden kann. Wenn nun Z nach dem Modul p^3 durch irgend einen Teiler von der Form $z+\alpha p$ teilbar ist, so wird

$$0 \equiv -\alpha p^2 Z'' + p^2 B \pmod{z+\alpha p,\ p^3} \quad \text{oder} \quad \alpha Z'' \equiv B \pmod{z,\ p}$$

sein. Nun können drei Fälle stattfinden.

1. Wenn $Z'' \equiv 0 \pmod{z,\ p}$ und B nicht $\equiv 0$ ist, so ist klar, dass kein Wert von α der Congruenz genügt und daher Z nach dem Modul p^3 keinen Teiler von der Form $z+\alpha p$ besitzt. Mithin ist die Untersuchung beendet.

2. Wenn weder Z'' noch $B \equiv 0$ (modd. z, p) ist, dann wird α einen einzigen Wert besitzen, nämlich:

$$\alpha \equiv \frac{B}{Z''} \text{ (modd. } z, p).$$

Mithin wird es einen einzigen Teiler $\equiv z + \alpha p$ (mod. p^2) von Z nach dem Modul p^3 geben und es wird sein:

$$Z \equiv V(z + \alpha p) + p^3 W.$$

Nimmt man nun als Teiler von Z (mod. p^4) $z + \alpha p + \beta p^2$ an, so ist:

$$0 \equiv$$

Weitere Entwicklung der Untersuchungen über die reinen Gleichungen.

1.

Da das Verfahren, nach welchem wir in den „*Arithmetischen Untersuchungen*“ Artikel 360 (vgl. oben S. 434) die Gleichung $x^n - 1 = 0$ lösen gelehrt haben, eine sehr fruchtbare und wichtige Theorie bildet, von welcher wir in jenem Werke nur die einfachsten Momente andeuten konnten, so wird es, hoffen wir, den Geometern angenehm sein, wenn wir diesen Gegenstand hier von Neuem aufnehmen, das, was nur kurz und zum Teil mit Unterdrückung der Beweise berührt worden ist, ausführlicher behandeln und die Erweiterungen, welche seit jener Zeit hinzugetreten sind, eingehender verfolgen.

Wir nehmen an, dass n eine Primzahl und die Zahl $n-1$ in die Factoren $\alpha \times \beta \times \gamma$ zerlegt sei, und bezeichnen ferner mit g irgend eine primitive Wurzel für den Modul n. Es stelle r unbestimmt eine Wurzel der Gleichung $x^n - 1 = 0$ und R unbestimmt eine Wurzel der Gleichung $x^\beta - 1 = 0$ dar. Bezeichnet man also die Peripherie des Kreises, dessen Radius gleich 1 ist, mit P und die imaginäre Grösse $\sqrt{-1}$ mit i, so werden sämtliche Wurzeln der Gleichung $x^\beta - 1 = 0$ oder sämtliche Werte von r dargestellt werden durch die Formel:

$$\cos\frac{kP}{\beta} + i\sin\frac{kP}{\beta},$$

wo k unbestimmt alle ganzen Zahlen $0, 1, 2, 3, \ldots, \beta - 1$ bezeichnet. Ferner ist klar, dass sämtliche Potenzen einer jeden Wurzel R ebenfalls Wurzeln sind, sowie dass, wenn R die einem zu β primen Werte von k entsprechende Wurzel ist, alle Potenzen $R^0, R, R^2, R^3, \ldots, R^{\beta-1}$ unter einander verschieden sind und daher den ganzen Complex der Wurzeln erschöpfen; in diesem Falle werden wir R eine **eigentliche Wurzel** der Gleichung $x^\beta - 1 = 0$ nennen; dagegen soll eine einem zu β nicht primen Werte von k entsprechende Wurzel R eine uneigentliche Wurzel heissen; und ist δ der grösste gemeinschaftliche Teiler der Zahlen k und β, so ist, wie leicht ersichtlich, $R^{\frac{\beta}{\delta}} = 1$,

ferner sind alle Potenzen $R^0, R, R^2, R^3, \ldots, R^{\frac{\beta}{\delta}-1}$ unter einander verschieden und daher R eine eigentliche Wurzel der Gleichung $x^{\frac{\beta}{\delta}} - 1 = 0$. Dasselbe gilt von der Gleichung $x^n - 1 = 0$, doch sind die Wurzeln dieser mit Ausnahme der Wurzel 1 notwendig sämtlich eigentliche Wurzeln.

2.

Nachdem dieses vorausgeschickt ist, soll nun unsere Untersuchung hauptsächlich handeln von den aus $\beta\gamma$ Gliedern bestehenden Functionen von folgender Form:

$$r + Rr^{g^\alpha} + R^2 r^{g^{2\alpha}} + R^3 r^{g^{3\alpha}} + \cdots + R^{\beta\gamma-1} r^{g^{\alpha\beta\gamma-\alpha}},$$

die wir der Kürze wegen mit folgendem Zeichen $[r, R]$ bezeichnen werden. Die einzelnen Glieder eines solchen Ausdrucks sind Producte aus Potenzen von r in Potenzen von R; die Exponenten jener bilden eine geometrische Reihe, die Exponenten dieser eine arithmetische Reihe. Die Exponenten

$$1,\ g^\alpha,\ g^{2\alpha},\ g^{3\alpha},\ \ldots,\ g^{\alpha\beta\gamma-\alpha}$$

sind alle nach dem Modul n incongruent und daher jene Potenzen von r unter einander verschieden; weiter fortgesetzt aber würden sie dieselbe Reihe von Neuem beginnen, da $g^{\alpha\beta\gamma} \equiv 1 \pmod{n}$ und daher $r^{g^{\alpha\beta\gamma}} \equiv r$ ist. Die andern Factoren

$$1,\ R,\ R^2,\ R^3,\ \ldots,\ R^{\beta\gamma-1}$$

aber bilden γ gleiche Perioden, da $R^\beta = 1$, $R^{\beta-1} = R$ u. s. w. ist. Hieraus geht hervor, dass die Function $[r, R]$ auch so dargestellt werden kann:

$$\begin{aligned} & r + r^{g^{\alpha\beta}} + r^{g^{2\alpha\beta}} + \cdots\cdots + r^{g^{\alpha\beta\gamma-\alpha\beta}} \\ & + R\,(r^{g^\alpha} + r^{g^{\alpha\beta+\alpha}} + r^{g^{2\alpha\beta+\alpha}} + \cdots\cdots + r^{g^{\alpha\beta\gamma-\alpha\beta+\alpha}}) \\ & + R^2(r^{g^{2\alpha}} + r^{g^{\alpha\beta+2\alpha}} + r^{g^{2\alpha\beta+2\alpha}} + \cdots\cdots + r^{g^{\alpha\beta\gamma-\alpha\beta+2\alpha}}) \\ & + \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ & + R^{\beta-1}(r^{g^{\alpha\beta-\alpha}} + r^{g^{2\alpha\beta-\alpha}} + r^{g^{3\alpha\beta-\alpha}} + \cdots\cdots + r^{g^{\alpha\beta\gamma-\alpha}}), \end{aligned}$$

oder mit Einführung des Zeichens im Artikel 343 der „*Arithmetischen Untersuchungen*" (vgl. oben S. 405):

$$[r, R] = (\gamma, 1) + R(\gamma, g^\alpha) + R^2(\gamma, g^{2\alpha}) + \cdots + R^{\beta-1}(\gamma, g^{\alpha\beta-\alpha}).$$

3.

Nehmen wir für die Wurzel r die Einheit, so erhalten wir:

$$\begin{aligned} [1, R] &= 1 + R + R^2 + R^3 + \cdots + R^{\beta\gamma-1} \\ &= \gamma(1 + R + R^2 + R^3 + \cdots + R^{\beta-1}), \end{aligned}$$

und der Wert dieses Ausdrucks ist $=\beta\gamma$, wenn auch für R die Wurzel 1 genommen wird, dagegen $=0$ für jeden andern Wert von R. Bleibt dagegen r unbestimmt und setzt man $R=1$, so ist:

$$[r, 1] = r + r^{g^\alpha} + r^{g^{2\alpha}} + r^{g^{3\alpha}} + \cdots + r^{g^{\alpha\beta\gamma-\alpha}},$$

oder mit Anwendung der in den „*Arithmetischen Untersuchungen*" eingeführten Bezeichnung: $[r, 1] = (\beta\gamma, 1)$, d. h. es wird $[r, 1]$ aus einer Periode von $\beta\gamma$ Wurzeln bestehen, von denen eine r selbst ist. Sooft $\alpha=1$ ist, wird diese Periode sämtliche Wurzeln $r, r^2, r^3, \ldots, r^{n-1}$ umfassen, nur in anderer Reihenfolge.

Man merke noch folgende Relationen, deren Grund von selbst einleuchtet:

$$[r, R] = R[r^{g^\alpha}, R] = R^2[r^{g^{2\alpha}}, R] \text{ oder allgemein } = R^k[r^{g^{\alpha k}}, R],$$

wo k eine beliebige positive ganze Zahl bezeichnet. Hieraus geht hervor, dass die Function $[r^m, R]$ entweder $=[1, R]$ ist, wenn nämlich m durch n teilbar ist, oder in den übrigen Fällen auf die Form $R^\mu[r^{g^\nu}, R]$ gebracht werden kann und zwar so, dass $\nu < \alpha$ ist. Denn wenn m nicht durch n teilbar ist, so wird es nach dem Modul n irgend einer Potenz von g, deren Exponent nach den „*Arithmetischen Untersuchungen*" passend durch ind. m dargestellt wird, congruent sein; setzt man daher ind. $m=\lambda\alpha+\nu$, was offenbar so geschehen kann, dass $\nu<\alpha$ ist, so ist:

$$[r^m, R] = [r^{g^{\lambda\alpha+\nu}}, R] = R^{-\lambda}[r^{g^\nu}, R];$$

man hat daher $\mu = -\lambda$ oder, wenn man einen positiven Exponenten haben will, $\mu \equiv -\lambda \pmod{\beta}$ zu setzen.

4.

Satz. Bezeichnet r' ebenso wie r unbestimmt eine Wurzel der Gleichung $x^n-1=0$, ferner R' ebenso wie R unbestimmt eine Wurzel der Gleichung $x^\beta-1=0$, so ist das Product

$$[r, R] \times [r', R'] = [rr', RR'] + R[r^{g^\alpha}r', RR'] + R^2[r^{g^{2\alpha}}r', RR'] + R^3[r^{g^{3\alpha}}r', RR'] + \cdots + R^{\beta\gamma-1}[r^{g^{\alpha\beta\gamma-\alpha}}r', RR'].$$

Beweis. Führt man die Multiplikation von $[r, R]$ mit den einzelnen Gliedern von $[r', R']$ aus, so lässt sich das Product in folgender Form darstellen:

$$[r, R]r' + RR'[r^{g^\alpha}, R]r'^{g^\alpha} + R^2R'^2[r^{g^{2\alpha}}, R]r'^{g^{2\alpha}} + R^3R'^3[r^{g^{3\alpha}}, R]r'^{g^{3\alpha}} + \cdots + R^{\beta\gamma-1}R'^{\beta\gamma-1}[r^{g^{\alpha\beta\gamma-\alpha}}, R]r'^{g^{\alpha\beta\gamma-\alpha}}.$$

Nimmt man sodann die ersten Glieder der einzelnen vorschriftsmässig entwickelten Teile zusammen, so ergiebt sich $[rr', RR']$; sammelt man ebenso die zweiten Glieder, so entsteht $R[r^{g^\alpha}r', RR']$ u. s. w., woraus man schliesslich die angegebene Form des Products erhält.

Ferner geht durch blosse Vertauschung von r, R mit r', R' hervor, dass dasselbe Product auch unter folgende Form gesetzt werden kann:

$$[rr', RR'] + R'[rr'^{g^\alpha}, RR'] + R'^2[rr'^{g^{2\alpha}}, RR'] + R'^3[rr'^{g^{3\alpha}}, RR'] + \cdots + R'^{\beta\gamma-1}[rr'^{g^{\alpha\beta\gamma-\alpha}}, RR'].$$

Hieraus folgt ferner, dass, wenn auch r'', r''', ... unbestimmt Wurzeln der Gleichung $x^n - 1 = 0$ sowie R'', R''', ... unbestimmt Wurzeln der Gleichung $x^\beta - 1 = 0$ sind, das Product aus den Functionen $[r, R]$, $[r', R']$, $[r'', R'']$, $[r''', R''']$, ..., wie gross auch ihre Anzahl sein möge, gleich dem Aggregate ist:

$$\Sigma R'^{k'} R''^{k''} R'''^{k'''} \dots [rr'^{g^{\alpha k'}} r''^{g^{\alpha k''}} r'''^{g^{\alpha k'''}} \dots, RR'R''R''' \dots],$$

wenn man für k', k'', k''', ... alle möglichen verschiedenen Combinationen der Zahlen $0, 1, 2, 3, \dots, \beta\gamma - 1$ setzt, wodurch sich im Ganzen $\beta^{\mu-1}\gamma^{\mu-1}$ Glieder ergeben werden, wenn mit μ die Anzahl jener mit einander multiplicierten Functionen bezeichnet wird.

5.

Die Formel, durch welche wir im vorigen Artikel das Product aus beliebig vielen Functionen dargestellt haben, ist allgemein und setzt keinen Zusammenhang zwischen den Wurzeln r, r', r'', r''', ... oder zwischen den Wurzeln R, R', R'', R''', ... voraus. Ohne Mühe leitet man hieraus her, dass, wenn die Wurzeln r', r'', r''', ... als Potenzen von r, die Wurzeln R', R'', R''', ... als Potenzen von R betrachtet werden dürfen, die einzelnen Teile des Products unter der Form $R^M[r^m, R^\lambda]$ enthalten sein werden, wo der Exponent λ für jeden einzelnen derselbe ist, nämlich $R^\lambda = RR'R''R'''\dots$ Daher reduciert sich nach dem, was wir im Artikel 3 angegeben haben, ein solches Product auf die folgende Form:

$$A[1, R^\lambda] + B[r, R^\lambda] + B'[r^g, R^\lambda] + B''[r^{g^2}, R^\lambda] + B'''[r^{g^3}, R^\lambda] + \cdots + B^{(\alpha-1)}[r^{g^{\alpha-1}}, R^\lambda],$$

wo die einzelnen Coefficienten A, B, B', B'', B''', ... von der Form sind:

$$h + h'R + h''R^2 + h'''R^3 + \cdots + h^{(\beta-1)}R^{\beta-1}$$

und h, h', h'', h''', ... bestimmte ganze Zahlen bezeichnen.

Der einfachste Fall ist der, wo $r = r' = r'' = r''' = \cdots$ sowie $R = R' = R'' = R''' = \cdots$ gesetzt wird; dann geht unser Product über in die Potenz $[r, R]^\lambda$, die somit stets auf die oben angegebene Form gebracht werden kann.

6.

Setzt man daher $\lambda = \beta$, so wird die Potenz $[r, R]^\beta$ folgende Form erhalten:

$$\begin{aligned} &A[1,1] + B[r,1] + B'[r^g, 1] + \cdots + B^{(\alpha-1)}[r^{g^{\alpha-1}}, 1] \\ = &A\beta\gamma + B(\beta\gamma, 1) + B'(\beta\gamma, g) + B''(\beta\gamma, g^2) + \cdots + B^{(\alpha-1)}(\beta\gamma, g^{\alpha-1}) \\ = &\vartheta'. \end{aligned}$$

Wenn demnach nicht nur der Wert der Wurzel R (und daher auch die Werte der Coefficienten A, B, B', ...), sondern auch die Werte der einzelnen Aggregate von $\beta\gamma$ Gliedern $(\beta\gamma, 1)$, $(\beta\gamma, g)$, ... als bekannt vorausgesetzt werden, so wird der Wert von ϑ' ohne Weiteres bekannt sein, so dass der Wert von $[r, R]$ mittelst der Formel $\sqrt[\beta]{\vartheta'}$ gefunden werden kann. Dieser Ausdruck lässt β verschiedene Werte zu, so dass es zweifelhaft erscheinen könnte, welchen man nehmen müsse; man zeigt aber leicht, dass dies völlig willkürlich ist, sobald R eine eigentliche Wurzel der Gleichung $x^\beta - 1 = 0$ ist. Denn in diesem Falle sind offenbar jene β Werte der Wurzelgrösse $\sqrt[\beta]{\vartheta'}$:

$$[r, R],\ [r^{g^\alpha}, R],\ [r^{g^{2\alpha}}, R],\ \ldots,\ [r^{g^{\alpha\beta-\alpha}}, R],$$

da die β^{ten} Potenzen dieser Functionen nach Artikel 3 unter einander gleich, sie selbst aber den β verschiedenen Wurzeln der Gleichung $x^\beta - 1 = 0$ proportional sind. Sobald aber nur die Aggregate von $\beta\gamma$ Gliedern $(\beta\gamma, 1)$, $(\beta\gamma, g)$, ... bekannt sind, ist die Wurzel r selbst nur insoweit bestimmt, als sie in dem Complexe $(\beta\gamma, 1)$ enthalten sein muss, und es bleibt willkürlich, welche wir aus diesem Complexe für r nehmen. Diese Wurzeln aber sind r, r^{g^α}, $r^{g^{2\alpha}}$, ..., und daher können wir auch von den Functionen $[r, R]$, $[r^{g^\alpha}, R]$, $[r^{g^{2\alpha}}, R]$, ... irgend eine für $[r, R]$ nehmen.

Diese Schlüsse würden nicht gelten, wenn R nicht eine eigentliche Wurzel der Gleichung $x^\beta - 1 = 0$ wäre. Denn nimmt man an, dass R eine eigentliche Wurzel der Gleichung $x^{\beta'} - 1 = 0$ sei, wo β' ein Teiler von β ist, so ergiebt sich leicht, dass

$$[r, R] = [r^{g^{\alpha\beta'}}, R],\ [r^{g^\alpha}, R] = [r^{g^{\alpha\beta'+\alpha}}, R],\ \ldots$$

wird und daher in dem Complex der β Functionen $[r, R]$, $[r^{g^\alpha}, R]$, ... $[r^{g^{\alpha\beta-\alpha}}, R]$ nur β' verschiedene vorkommen, also auch von den Werten des Ausdrucks $\sqrt[\beta]{\vartheta'}$ nicht mehr als β' zulässig, die übrigen $\beta - \beta'$ aber zu verwerfen sind. Man sieht aber leicht, dass man in diesem Falle nicht bis zur β^{ten} Potenz der Function $[r, R]$ aufzusteigen braucht, sondern dass schon die Potenz $[r, R]^{\beta'}$ sich auf unsere Form

$$\beta\gamma A + B(\beta\gamma, 1) + B'(\beta\gamma, g) + B''(\beta\gamma, g^2) + \cdots$$

reduciert. Wir erhalten daher $[r, R]$ durch einen Ausdruck wie $\sqrt[\beta']{\vartheta}$, und es ist gleichgültig, welchen Wert dieses Ausdrucks wir nehmen.

7.

Ebenso wie $[r, R]$ kann man auch die Funktionen $[r, R^2]$, $[r, R^3]$, ... oder allgemein $[r, R^k]$ bestimmen; denn offenbar wird, wenn man annimmt, dass durch Substitution der Potenzen R^2, R^3, ..., R^k an Stelle von R in ϑ' die Functionen ϑ'', ϑ''', ..., $\vartheta^{(k)}$ entstehen, $[r, R^2]^\beta = \vartheta''$, $[r, R^3]^\beta = \vartheta'''$, ... und allgemein $[r, R^k]^\beta = \vartheta^{(k)}$ sein, weshalb auch diese Functionen durch Wurzelgrössen dargestellt werden können, $[r, R^2] = \sqrt[\beta]{\vartheta''}$, u. s. w. Indessen ist es nicht zweckmässig, sich dieser Wurzelausdrücke zu bedienen, sobald irgend eine Grösse durch eine Function von $[r, R]$, $[r, R^2]$, ... auszudrücken ist. Da nämlich die Werte der einzelnen nicht vollständig bestimmt sind, so würde es zweifelhaft bleiben, welche man unter einander combinieren könnte; offenbar aber ist dies keineswegs willkürlich; denn man sieht leicht, dass, sobald für $[r, R]$ ein bestimmter Wert genommen wird, auch alle Functionen $[r, R^2]$, $[r, R^3]$, ... völlig bestimmte Werte erhalten müssen, die aber durch die Wurzelgrössen nicht angezeigt werden. Man hat daher diese zu verwerfen und andere Ausdrücke zu ermitteln, mit deren Hülfe $[r, R^2]$, $[r, R^3]$, ... rational durch $[r, R]$ und bekannte Grössen dargestellt werden, was wir leicht auf folgende Weise bewirken.

Nach dem Satze des Artikels 4 und nach dem, was wir im Artikel 5 dargelegt haben, lässt sich auch das Product $[r, R^k] \times [r, R]^{\beta-k}$ auf eine solche Form

$$\beta\gamma A + B(\beta\gamma, 1) + B'(\beta\gamma, g) + B''(\beta\gamma, g^2) + \cdots + B^{(\alpha-1)}(\beta\gamma, g^{\alpha-1})$$

bringen, wo A, B, B', B'', ... rationale Functionen von R sein werden. Setzt man daher die Producte

$$[r, R^2] \times [r, R]^{\beta-2} = \vartheta''$$
$$[r, R^3] \times [r, R]^{\beta-3} = \vartheta'''$$
$$[r, R^4] \times [r, R]^{\beta-4} = \vartheta''''$$
u. s. w.,

so werden auch ϑ'', ϑ''', ϑ'''', ... rational angebbare Grössen und

$$[r, R^2] = \frac{\vartheta''}{\vartheta'}[r, R]^2$$
$$[r, R^3] = \frac{\vartheta'''}{\vartheta'}[r, R]^3$$
$$[r, R^4] = \frac{\vartheta''''}{\vartheta'}[r, R]^4$$
u. s. w.

sein. Diese Ausdrücke stellen somit die Werte der Functionen $[r, R^2]$, $[r, R^3]$, ... rational dar, wofern nicht $[r, R] = 0$ ist, in welchem Falle sie unbestimmt werden; wir können aber streng beweisen, dass niemals $[r, R] = 0$

werden kann, sooft wenigstens r eine von 1 verschiedene Wurzel bezeichnet, obwohl wir die Darlegung dieses Beweises, um nicht hier allzu weitläufig zu werden, uns auf eine andere Gelegenheit vorbehalten müssen.

8.

Die Auseinandersetzungen des vorigen Artikels sind vorteilhaft, wenn die Aufgabe gestellt ist, von den Perioden von $\beta\gamma$ Gliedern zu den Perioden von γ Gliedern herabzusteigen. Denn man sieht leicht, dass man, wenn R eine eigentliche Wurzel bezeichnet, erhält:

$$\beta(\gamma, 1) = (\beta\gamma, 1) + [r, R] + [r, R^2] + [r, R^3] + \cdots + [r, R^{\beta-1}]$$

$$\beta(\gamma, g^\alpha) = (\beta\gamma, 1) + R^{\beta-1}[r, R] + R^{\beta-2}[r, R^2] + R^{\beta-3}[r, R^3] + \cdots + R[r, R^{\beta-1}]$$

$$\beta(\gamma, g^{2\alpha}) = (\beta\gamma, 1) + R^{2\beta-2}[r, R] + R^{2\beta-4}[r, R^2] + R^{2\beta-6}[r, R^3] + \cdots + R^2[r, R^{\beta-1}]$$

u. s. w.

Wenn hier für die einzelnen $[r, R]$, $[r, R^2]$, ... die Wurzelausdrücke $\sqrt[\beta]{\vartheta'}$, $\sqrt[\beta]{\vartheta''}$, ... genommen würden, so würde der Wert einer jeden Reihe unter $\beta^{\beta-1}$ Werten zweifelhaft sein, während er doch, wenn man die rationalen Ausdrücke für $[r, R^2]$, ... nimmt, keiner andern Zweideutigkeit unterworfen ist, als derjenigen, welche der Natur der Sache nach unvermeidlich ist. Diese Bemerkung scheint der Aufmerksamkeit Lagrange's entgangen zu sein, der unsere in den *„Arithmetischen Untersuchungen“* Artikel 360 angeführte Methode, bei der wir nicht ohne Vorbedacht mit Übergehung von Wurzelausdrücken nur rationale Ausdrücke angegeben hatten, vereinfacht zu haben glaubte, während er jene für diese substituierte. *(Traité de la résolution numérique des équations; édition 2ième, page 311.)*

Ferner dürfte es kaum nötig sein, darauf hinzuweisen, dass, sobald die Werte der Perioden $(\gamma, 1)$, (γ, g^α), ... oder nur einer von ihnen ermittelt sind, die Werte aller übrigen Perioden von γ Gliedern rational daraus hergeleitet werden können. Mithin erfordert das Absteigen von Perioden mit $\beta\gamma$ Gliedern auf Perioden von γ Gliedern die Auflösung der Gleichungen $x^\beta = 1$, $x^\beta = \vartheta'$, und alle übrigen Operationen werden rational ausgeführt.

9.

Alles dies war fast auf dieselbe Weise in den *„Arithmetischen Untersuchungen“* behandelt worden; einiges aber war dort mit Unterdrückung des Beweises, den hier nachzutragen nicht unangebracht sein dürfte, mitgeteilt worden. Wir haben daselbst behauptet, dass die Entwicklung des Wertes der Wurzelgrösse $\sqrt[\beta]{\vartheta'}$, welche, wenigstens wenn ϑ' eine imaginäre Grösse ist, die Teilung sowohl eines Verhältnisses als auch eines Winkels

in β Teile zu erfordern scheint, nur von der letzteren abhängt und die erstere immer auf die Ausziehung einer einzigen Quadratwurzel reduciert werden kann. Dies beweisen wir folgendermaassen.

Bezeichnet man wie oben die imaginäre Grösse $\sqrt{-1}$ mit i und setzt man $\vartheta' = P + iQ$ und irgend einen Wert des Ausdrucks $\sqrt[\beta]{\vartheta'} = p + iq$, so dass P, Q, p, q reell sind, so ist bekanntlich, wenn die positiven Grössen E, e und die Winkel F, f so bestimmt werden, dass

$$P = E\cos F,\ Q = E\sin F,\ p = e\cos f,\ q = e\sin f$$

ist,

$$e = \sqrt[\beta]{E}$$

und f gleich irgend einem der Winkel:

$$\frac{1}{\beta}F,\ \frac{1}{\beta}(F + 360^\circ),\ \frac{1}{\beta}(F + 720^\circ), \ldots,\ \frac{1}{\beta}\big(F + (\beta - 1)360^\circ\big).$$

Es wird daher f durch die Teilung des Winkels F in β Teile bestimmt werden, der Ausziehung der Wurzel $\sqrt[\beta]{E}$ aber können wir in folgender Weise aus dem Wege gehen. Jedes Product $r^k R^K$ hat seinen reellen Teil gemeinschaftlich mit $r^{-k}R^{-K}$, die imaginären Teile aber, welche den Factor i enthalten, sind in diesen Producten gleich aber von entgegengesetztem Vorzeichen. Hieraus folgt unmittelbar:

$$[r^{-1}, R^{-1}] = p - iq = e(\cos f - i\sin f)$$

und daher:

$$[r, R] \times [r^{-1}, R^{-1}] = e^2.$$

Jenes Product wird aber nach dem Satze des Artikels 4:

$$\begin{aligned} &= [1, 1] + R[r^{g^\alpha - 1}, 1] + R^2[r^{g^{2\alpha}-1}, 1] + \cdots\cdots + R^{\beta\gamma-1}[r^{g^{\alpha\beta\gamma-\alpha}-1}, 1] \\ &= \beta\gamma + R(\beta\gamma, g^\alpha - 1) + R^2(\beta\gamma, g^{2\alpha} - 1) + \cdots\cdots + R^{\beta\gamma-1}(\beta\gamma, g^{\alpha\beta\gamma-\alpha} - 1), \end{aligned}$$

welche Grösse bestimmbar ist, wenn R und alle Perioden von $\beta\gamma$ Gliedern als bekannt vorausgesetzt werden. Die Bestimmung von e erfordert also nur die Ausziehung einer Quadratwurzel.

In dem speciellen Falle, wo $\alpha = 1$ ist, sind die einzelnen Perioden $(\beta\gamma, g^\alpha - 1), (\beta\gamma, g^{2\alpha} - 1), \ldots.$ offenbar gleich $r + r^2 + r^3 + r^4 + \cdots\cdot + r^{n-1}$ und daher:

$$\begin{aligned} e^2 &= \beta\gamma + (R + R^2 + R^3 + \cdots + R^{\beta\gamma-1})(r + r^2 + r^3 + \cdots + r^{n-1}) \\ &= \beta\gamma + 1 = n, \end{aligned}$$

wenn man annimmt, dass r und R von 1 verschiedene Wurzeln darstellen, und somit stets $e = \sqrt{n}$ („*Arithmetische Untersuchungen*“ Artikel 360 am Ende, vgl. oben S. 437).

10.

Bisher haben wir unsere Untersuchung in grösster Allgemeinheit geführt, so dass sie beliebige Werte der Zahlen α, β, γ umfasst; von jetzt aber werden wir zu dem specielleren Falle, wo $\alpha = 1$ ist, und der uns den Weg zu den fruchtbarsten und elegantesten Untersuchungen bahnen wird, übergehen. Es stelle daher das Zeichen $[r, R]$ die Function dar:

$$r + Rr^g + R^2 r^{g^2} + R^3 r^{g^3} + \cdots + R^{n-2} r^{g^{n-2}}$$

wo n eine Primzahl, r unbestimmt eine Wurzel der Gleichung $x^n - 1 = 0$ (die Wurzel 1 nicht ausgenommen), R unbestimmt eine Wurzel der Gleichung $x^\beta - 1 = 0$ ist; hierin bezeichnet β einen gegebenen Teiler von $n-1$, endlich g eine ganze Zahl, welche eine bestimmte primitive Wurzel für den Modul n ist. Ferner setzen wir der Kürze halber

$$1 + r + r^2 + r^3 + \cdots + r^{n-1} = s$$
$$1 + R + R^2 + R^3 + \cdots + R^{n-2} = S,$$

woraus hervorgeht, dass $s = n$ wird für $r = 1$ und $= 0$ für jeden andern Wert von r, und ebenso $S = n-1$ für $R = 1$, aber $S = 0$ für jeden andern Wert von R.

Nach Artikel 3 haben wir somit:

$$[1, R] = S, \quad [r, 1] = s - 1;$$

ferner für jeden durch n nicht teilbaren ganzen Wert von m:

$$[r^m, R] = R^{-\operatorname{ind}.m}[r, R],$$

oder allgemeiner:

$$[r^m, R^M] = R^{-M\operatorname{ind}.m}[r, R^M],$$

wo $\operatorname{ind}.m$ der Exponent einer nach dem Modul n zu m congruenten Potenz der Zahl g ist. Wendet man diese Transformation auf das an, was wir im Artikel 5 dargelegt haben, so folgt, dass das Product aus zwei oder mehr solchen Factoren wie $[r^h, R^H]$ auf die Form sich reduciert:

$$A[1, R^\lambda] + B[r, R^\lambda],$$

wo A und B rationale Functionen von R mit ganzzahligen Coefficienten sind und λ das Aggregat aller Werte von H ist. Von grosser Wichtigkeit wird es sein, derartige Transformationen auf einen einfachen Algorithmus zurückzuführen, zu welchem Zwecke wir insbesondere die Natur des Products aus zwei Functionen näher betrachten müssen.

11.

Das Product $[r, R^\mu] \times [r, R^\nu]$ wird nach dem Satze des Artikels 4 gleich

$$[r^2, R^{\mu+\nu}] + R^\mu[r^{g+1}, R^{\mu+\nu}] + R^{2\mu}[r^{g^2+1}, R^{\mu+\nu}] + R^{3\mu}[r^{g^3+1}, R^{\mu+\nu}] + \cdots$$
$$+ R^{(n-2)\mu}[r^{g^{n-2}+1}, R^{\mu+\nu}]$$

Unter den $n-1$ Exponenten $2, g+1, g^2+1, g^3+1, \ldots, g^{n-2}+1$ kommt nur einer vor, der durch n teilbar ist, nämlich $g^{\frac{1}{2}(n-1)}+1$; das entsprechende Glied unseres Aggregates wird also sein:

$$R^{\frac{1}{2}(n-1)\mu}[1, R^{\mu+\nu}];$$

dieses Glied ist gleich 0, sobald $R^{\mu+\nu}$ nicht gleich 1 ist, und gleich $(n-1)R^{\frac{1}{2}(n-1)\mu} = \pm(n-1)$ für $R^{\mu+\nu}=1$. Die übrigen Teile unseres Aggregates, deren Summe wir gleich Ω setzen, werden in folgender Weise transformiert:

$$\begin{aligned}
[r^2, R^{\mu+\nu}] &= R^{-(\mu+\nu)\,\mathrm{ind.}\,2}[r, R^{\mu+\nu}]\\
R^{\mu}[r^{g+1}, R^{\mu+\nu}] &= R^{\mu-(\mu+\nu)\,\mathrm{ind.}\,(g+1)}[r, R^{\mu+\nu}]\\
R^{2\mu}[r^{g^2+1}, R^{\mu+\nu}] &= R^{2\mu-(\mu+\nu)\,\mathrm{ind.}\,(g^2+1)}[r, R^{\mu+\nu}]\\
R^{3\mu}[r^{g^3+1}, R^{\mu+\nu}] &= R^{3\mu-(\mu+\nu)\,\mathrm{ind.}\,(g^3+1)}[r, R^{\mu+\nu}]
\end{aligned}$$

u. s. w.

Hieraus folgt:

I. $$\Omega = [r, R^{\mu+\nu}] \times \Sigma R^{\mu\,\mathrm{ind.}\,x-(\mu+\nu)\,\mathrm{ind.}\,(x+1)},$$

wenn für x der Reihe nach die Werte $1, g, g^2, g^3, \ldots, g^{n-2}$, den einen $g^{\frac{1}{2}(n-1)}$ ausgenommen, substituiert werden, oder, was dasselbe ist, wenn für x die Werte $1, 2, 3, 4, \ldots, n-2$ substituiert werden, da diese Werte jenen (wenn auch in anderer Reihenfolge) nach dem Modul n congruent sind.

Nehmen wir an, dass die ganze Zahl y zu x nach dem Modul n reciprok d. h. so bestimmt sei, dass $xy \equiv 1 \pmod{n}$ ist, so wird $\mathrm{ind.}\,x \equiv -\mathrm{ind.}\,y \pmod{n-1}$ und

$$\mathrm{ind.}\,(x+1) + \mathrm{ind.}\,y \equiv \mathrm{ind.}\,(xy+y) \equiv \mathrm{ind.}\,(1+y) \pmod{n-1}.$$

Daher wird

$$\begin{aligned}
\mu\,\mathrm{ind.}\,x-(\mu+\nu)\,\mathrm{ind.}\,(x+1) &\equiv -\mu\,\mathrm{ind.}\,y-(\mu+\nu\{\mathrm{ind.}\,(y+1)-\mathrm{ind.}\,y\}\\
&\equiv \nu\,\mathrm{ind.}\,y-(\mu+\nu)\,\mathrm{ind.}\,(y+1).
\end{aligned}$$

Demnach ist auch, da die zu $1, 2, 3, \ldots, n-2$ reciproken Zahlen mit diesen, nur in anderer Reihenfolge genommen, übereinstimmen.

II. $$\Omega = [r, R^{\mu+\nu}] \times \Sigma R^{\nu\,\mathrm{ind.}\,y-(\mu+\nu)\,\mathrm{ind.}\,(y+1)},$$

wenn man für y der Reihe nach die Zahlen $1, 2, 3, \ldots, n-2$ substituiert. Ebendieselbe Formel geht unmittelbar aus I. hervor, da offenbar die Zahlen μ, ν unter einander vertauscht werden können.

Nimmt man endlich an, dass die ganze Zahl z zu $x+1$ nach dem Modul n reciprok oder $xz+z\equiv 1 \pmod{n}$ sei, so ist:

$$\begin{aligned}
\mathrm{ind.}\,(1-z) &\equiv \mathrm{ind.}\,x+\mathrm{ind.}\,z \pmod{n-1},\\
\mathrm{ind.}\,(x+1) &\equiv -\mathrm{ind.}\,z \pmod{n-1},
\end{aligned}$$

und daher:

$$\begin{aligned}\mu \operatorname{ind.} x - (\mu + \nu) \operatorname{ind.} (x+1) &\equiv \mu [\operatorname{ind.} (1-z) - \operatorname{ind.} z] + (\mu+\nu) \operatorname{ind.} z \\ &\equiv \mu \operatorname{ind.} (1-z) + \nu \operatorname{ind.} z.\end{aligned}$$

Wir erhalten somit, da, wenn x die Werte 1, 2, 3, ..., $n-2$ durchläuft, die Zahl z die Werte 2, 3, 4, ..., $n-1$ durchlaufen muss (wenn auch in anderer Reihenfolge), den dritten Ausdruck:

$$\text{III.} \qquad \Omega = [r, R^{\mu+\nu}] \times \Sigma R^{\mu \operatorname{ind.}(1-z)+\nu \operatorname{ind.} z},$$

wenn wir der Reihe nach für z die Werte 2, 3, 4, ..., $n-1$ setzen, oder wenn man lieber will:

$$\begin{aligned}\Omega &= [r, R^{\mu+\nu}] \times \Sigma R^{\mu \operatorname{ind.}(n+1-z)+\nu \operatorname{ind.} z} \\ &= [r, R^{\mu+\nu}] \times \Sigma R^{\mu \operatorname{ind.} z+\nu \operatorname{ind.}(n+1-z)}.\end{aligned}$$

Da man $\operatorname{ind.}(1-z) = \frac{1}{2}(n-1) + \operatorname{ind.}(z-1)$ hat, so kann man unser Product auch so darstellen:

$$\begin{aligned}[r, R^{\mu}] \times [r, R^{\nu}] &= R^{\frac{1}{2}(n-1)\mu}\{[1, R^{\mu+\nu}] + [r, R^{\mu+\nu}] \times \Sigma R^{\mu \operatorname{ind.}(z-1)+\nu \operatorname{ind.} z}\} \\ &= R^{\frac{1}{2}(n-1)\nu}\{[1, R^{\mu+\nu}] + [r, R^{\mu+\nu}] \times \Sigma R^{\mu \operatorname{ind.} z+\nu \operatorname{ind.}(z-1)}\},\end{aligned}$$

wo stets die für z zu substituierenden Werte 2, 3, 4, ..., $n-1$ sind.

Übrigens kann man in allen diesen Formeln für die Zahlen

$$\mu \operatorname{ind.} x - (\mu+\nu) \operatorname{ind.}(x+1), \quad \nu \operatorname{ind.} y - (\mu+\nu) \operatorname{ind.}(y+1), \quad \mu \operatorname{ind.}(1-z) + \nu \operatorname{ind.} z, \text{ u. s. w.}$$

offenbar ihre kleinsten Reste nach dem Modul β substituieren.

Wenn $\mu + \nu \equiv 0 \pmod{\beta}$ ist, so ist

$$\begin{aligned}[r, R^{\mu}] \times [r, R^{\nu}] = (n-1) R^{\frac{1}{2}(n-1)\mu} &+ (r + r^2 + r^3 + \cdots + r^{n-1}) \\ &\times (1 + R^{\mu} + R^{2\mu} + R^{3\mu} + \cdots + R^{(n-2)\mu} - R^{\frac{1}{2}(n-1)\mu}).\end{aligned}$$

12.

Das Product $[1, R^{\mu}] \times [r, R^{\nu}]$ wird nach dem Satze des Artikels 4:

$$\begin{aligned}&= [r, R^{\mu+\nu}] + R^{\mu}[r, R^{\mu+\nu}] + R^{2\mu}[r, R^{\mu+\nu}] + \cdots + R^{(n-2)\mu}[r, R^{\mu+\nu}] \\ &= [r, R^{\mu+\nu}] \times (1 + R^{\mu} + R^{2\mu} + R^{3\mu} + \cdots + R^{(n-2)\mu}) \\ &= [r, R^{\mu+\nu}] \times \frac{n-1}{\beta}(1 + R^{\mu} + R^{2\mu} + R^{3\mu} + \cdots + R^{(\beta-1)\mu}).\end{aligned}$$

Hiernach lässt sich das Product $[1, R^{\mu}] \times [1, R^{\nu}]$ entwickeln in

$$\frac{n-1}{\beta}[1, R^{\mu+\nu}] \times (1 + R^{\mu} + R^{2\mu} + R^{3\mu} + \cdots + R^{(\beta-1)\mu}).$$

Nunmehr kann man ohne Mühe allgemein das Product $[r^m, R^\mu] \times [r^{m'}, R^{\mu'}]$ ermitteln; denn da $[r^m, R^\mu] = R^{-\mu\,\mathrm{ind}.m}[r, R^\mu]$ für einen durch n nicht teilbaren Wert von m und $= [1, R^\mu]$ für einen durch n teilbaren Wert von m wird, und da eine ähnliche Transformation für den andern Factor $[r^{m'}, R^{\mu'}]$ gilt, so reduciert sich die Multiplikation entweder auf die Aufgabe des vorigen Artikels oder auf diejenigen Fälle, die wir im gegenwärtigen Artikel betrachtet haben.

13.

Nachdem wir gezeigt haben, wie man das Product aus zwei Factoren entwickelt, wird die Entwicklung eines Products aus mehreren Factoren keiner Schwierigkeit unterliegen. Ist das Product $[r, R^\mu] \times [r, R^\nu]$ auf die Form $A[1, R^{\mu+\nu}] + B[r, R^{\mu+\nu}]$ gebracht, so ist klar, dass, wenn ein dritter Factor $[r, R^\pi]$ hinzutritt, das Product $= C[1, R^{\mu+\nu+\pi}] + D[r, R^{\mu+\nu+\pi}]$ werden wird, wenn man setzt:

$$[r, R^{\mu+\nu}] \times [r, R^\pi] = c[1, R^{\mu+\nu+\pi}] + d[r, R^{\mu+\nu+\pi}]$$

und

$$C = Bc$$

$$D = Bd + A\left\{1 + R^{\mu+\nu} + R^{2\mu+2\nu} + \cdots + R^{(n-2)(\mu+\nu)}\right\}.$$

Hiernach kann $[r, R]^\lambda$ leicht auf die Form $A[1, R^\lambda] + B[r, R^\lambda]$ gebracht werden.

Beispielshalber wollen wir die Potenzen der Function $[r, R]$ für $n = 11$, $\beta = 5$ entwickeln, wobei wir $g = 2$ setzen. Hiernach entsprechen

den Zahlen:	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,
die Indices:	0,	1,	8,	2,	4,	9,	7,	3,	6,	5.

Wir haben daher zur Entwicklung des Quadrats $[r, R]^2$ nach Formel I im Artikel 11:

$$\mu = 1,\ \nu = 1$$

Werte von x	1.	2.	3.	4.	5.	6.	7.	8.	9.
ind. x	0.	1.	8.	2.	4.	9.	7.	3.	6.
2 ind. $(x+1)$	2.	16.	4.	8.	18.	14.	6.	12.	10.
Kl. Rest von ind. x — 2 ind. $(x+1)$ (mod. 5)	3.	0.	4.	4.	1.	0.	1.	1.	1,

woraus wir erhalten:

$$\Omega = [r, R^2] \times \left\{2 + 4R + R^3 + 2R^4\right\}$$

und

1) $\quad [r, R]^2 = [1, R^2] + [r, R^2] \times \left\{2 + 4R + R^3 + 2R^4\right\}.$

Ebenderselbe Ausdruck ergiebt sich aus Formel III des Artikels 11, nämlich:

Werte von z	2.	3.	4.	5.	6.	7.	8.	9.	10.
ind. z	1.	8.	2.	4.	9.	7.	3.	6.	5.
ind. $(n+1-z)$	5.	6.	3.	7.	9.	4.	2.	8.	1.
Kl. Rest von ind. z + ind. $(n+1-z)$ (mod. 5)	1.	4.	0.	1.	3.	1.	0.	4.	1.

Auf ganz analoge Weise findet man:

$$2)\ [r, R^2]\times[r, R] = [1, R^3] + [r, R^3]\times\{2 + R + 4R^2 + 2R^3\}$$

$$3)\ [r, R^3]\times[r, R] = [1, R^4] + [r, R^4]\times\{2 + 4R + R^3 + 2R^4\}.$$

Endlich wird:

$$4)\ [r, R^4]\times[r, R] = [1, 1] + [r, 1]\times\{1 + 2R + 2R^2 + 2R^3 + 2R^4\}.$$

Multipliciert man die Gleichung 1) mit $[r, R]$ und substituiert man für $[r, R^2]\times[r, R]$ seinen Wert aus 2) sowie ferner

$$[1, R^2]\times[r, R] = [r, R^3]\times\{2 + 2R + 2R^2 + 2R^3 + 2R^4\},$$

so leitet man hieraus die Gleichung her:

$$\begin{aligned}[r, R]^3 = {} & [1, R^3]\times\{2 + 4R + R^3 + 2R^4\} \\ & + [r, R^3]\times\{12 + 22R + 18R^2 + 24R^3 + 15R^4\}\end{aligned}$$

und ebenso:

$$\begin{aligned}[r, R]^4 = {} & [1, R^4]\times\{12 + 22R + 18R^2 + 24R^3 + 15R^4\} \\ & + [r, R^4]\times\{164 + 170R + 205R^2 + 180R^3 + 190R^4\} \\ [r, R]^5 = {} & [1, 1]\ \times\{164 + 170R + 205R^2 + 180R^3 + 190R^4\} \\ & + [r, 1]\ \times\{1836 + 1830R + 1795R^2 + 1820R^3 + 1810R^4\} \\ = {} & 1640 + 1700R + 2050R^2 + 1800R^3 + 1900R^4 \\ & + (1836 + 1830R + 1795R^2 + 1820R^3 + 1810R^4)(s-1) \\ = {} & 918Ss - 98S - (6R + 41R^2 + 16R^3 + 26R^4)s \\ & \qquad + 66R + 451R^2 + 176R^3 + 286R^4.\end{aligned}$$

14.

Die Rechnung, welche im Vorhergehenden in der Weise durchgeführt ist, dass sie auf alle Werte von r und R ausgedehnt werden kann, lässt sich beträchtlich zusammenziehen, wenn wir R gleich von Anfang an als eigentliche Wurzel der Gleichung $x^\beta - 1 = 0$ betrachten. Unter dieser Voraussetzung reduciert sich das Product $[r, R^\mu]\times[r, R^\nu]$ auf die Form $B[r, R^{\mu+\nu}]$, sobald $\mu+\nu$ durch β nicht teilbar ist. Ist aber $\mu+\nu$ durch β teilbar, so wird jenes Product gleich $(n-1)R^{\frac{1}{2}(n-1)\mu} + [r, 1]\Sigma R^{\mu\,\mathrm{ind.}\,x}$, wenn man für ind. x alle Werte $0, 1, 2, 3, \ldots, n-2$ mit Ausnahme von $\frac{1}{2}(n-1)$ substituiert. Hieraus folgt leicht (wenn μ und somit auch ν durch β nicht teilbar ist), dass in diesem Falle ist:

$$[r, R^\mu]\times[r, R^\nu] = R^{\frac{1}{2}(n-1)\mu}\{n - 1 - [r, 1]\}$$

und daher $= 0$ für $r = 1$ und $= nR^{\frac{1}{2}(n-1)\mu}$ für jeden andern Wert von r. Da ferner $R^{\frac{1}{2}(n-1)\mu} = +1$ oder $= -1$ wird, je nachdem $\frac{n-1}{\beta}\cdot\mu$ eine gerade oder ungerade Zahl ist, so wird unser Product im ersteren Falle $= n$, im letzteren $= -n$.

Ferner folgt hieraus, dass man

$$\begin{aligned} [r, R]^2 &= A' \; [r, R^2] \\ [r, R^2] \times [r, R] &= A'' \; [r, R^3] \\ [r, R^3] \times [r, R] &= A''' [r, R^4] \\ &\cdots\cdots\cdots \\ [r, R^{\beta-2}] \times [r, R] &= A^{(\beta-2)} [r, R^{\beta-1}] \end{aligned}$$

setzen kann, wodurch man erhält:

$$\begin{aligned} [r, R]^2 &= A' [r, R^2] \\ [r, R]^3 &= A'A'' [r, R^3] \\ [r, R]^4 &= A'A''A''' [r, R^4] \end{aligned}$$

u. s. w.

endlich:

$$[r, R]^\beta = \pm n A'A''A''' \ldots A^{(\beta-2)},$$

wo das obere oder untere Vorzeichen zu nehmen ist, je nachdem $\frac{n-1}{\beta}$ gerade oder ungerade ist.

Hieraus geht also hervor, dass, nachdem der Wert von $[r, R]$ gefunden ist, die übrigen Functionen

$$[r, R^2] = \frac{[r, R]^2}{A'}, \quad [r, R^3] = \frac{[r, R]^3}{A'A''}, \ldots$$

hier viel leichter bestimmt werden können, als in denjenigen Fällen, wo α nicht gleich 1 ist, worauf wir schon in den „*Arithmetischen Untersuchungen*" (Artikel 360, III vgl. oben S. 437) hingewiesen haben. Durch eine eingehendere Betrachtung der Natur der Functionen A', A'', ... lassen sich diese Operationen noch mehr vereinfachen.

15.

Im Artikel 9 haben wir gezeigt, dass der Wert der Function $[r, R]$ auf die Form $\sqrt{n}(\cos f + i \sin f)$ gebracht werden kann, und auf dieselbe Weise werden sich die Functionen $[r, R^2]$, $[r, R^3]$ u. s. w. bis zu $[r, R^{\beta-1}]$ auf eine ähnliche Form bringen lassen. Setzen wir:

$$\begin{aligned} [r, R] &= \sqrt{n}(\cos f' + i \sin f') \\ [r, R^2] &= \sqrt{n}(\cos f'' + i \sin f'') \\ [r, R^3] &= \sqrt{n}(\cos f''' + i \sin f''') \end{aligned}$$

u. s. w.,

so wird:

$$\begin{aligned} A' &= \sqrt{n}[\cos(2f' - f'') + i \sin(2f' - f'')] \\ A'' &= \sqrt{n}[\cos(f' + f'' - f''') + i \sin(f' + f'' - f''')] \\ A''' &= \sqrt{n}[\cos(f' + f''' - f'''') + i \sin(f' + f''' - f'''')] \end{aligned}$$

u. s. w.

Bringt man die Functionen $A', A'', A''', \ldots$ auf die Formen

$$\begin{aligned} A' &= a'\,(\cos b' + i\sin b') \\ A'' &= a''\,(\cos b'' + i\sin b'') \\ A''' &= a'''(\cos b''' + i\sin b''') \\ &\text{u. s. w.,} \end{aligned}$$

und zwar so, dass alle $a', a'', a''', \ldots$ positiv sind, so ergiebt sich hieraus, dass

$$a' = a'' = a''' = \cdots = \sqrt{n}$$
$$f' = \frac{1}{\beta}(b' + b'' + b''' + \cdots + b^{(n-2)})$$

ist, wenn $\frac{n-1}{\beta}$ gerade, oder

$$f' = \frac{1}{\beta}(180° + b' + b'' + b''' + \cdots + b^{(n-2)}),$$

wenn $\frac{n-1}{\beta}$ ungerade ist, und sodann

$$\begin{aligned} [r, R] &= \sqrt{n}(\cos f' + i\sin f') \\ [r, R^2] &= \sqrt{n}\big(\cos(2f' - b') + i\sin(2f' - b')\big) \\ [r, R^3] &= \sqrt{n}\big(\cos(3f' - b' - b'') + i\sin(3f' - b' - b'')\big) \\ &\text{u. s. w.} \end{aligned}$$

Endlich ist nach den Formeln des Artikels 8:

$$\begin{aligned} \left(\frac{n-1}{\beta}, 1\right) = -\frac{1}{\beta} + \frac{\sqrt{n}}{\beta}\{&\cos f' + \cos(2f' - b') + \cos(3f' - b' - b'') + \cdots \\ &+ \cos\big((\beta-1)f' - b' - b'' - b''' - \cdots - b^{(\beta-2)}\big)\} \\ + \frac{i\sqrt{n}}{\beta}\{&\sin f' + \sin(2f' - b') + \sin(3f' - b' - b'') + \cdots \\ &+ \sin\big((\beta-1)f' - b' - b'' - b''' - \cdots - b^{(\beta-2)}\big)\}, \end{aligned}$$

und ebenso ergeben sich die Werte der Functionen $\left(\frac{n-1}{\beta}, g\right), \left(\frac{n-1}{\beta}, g^2\right), \left(\frac{n-1}{\beta}, g^3\right), \ldots$, wenn man in dieser Formel für f' respective $f' - \frac{360°k}{\beta}$, $f' - 2\frac{360°k}{\beta}$, $f' - 3\frac{360°k}{\beta}$, ... substituiert, wobei $R = \cos\frac{360°k}{\beta} + i\sin\frac{360°k}{\beta}$ vorausgesetzt ist.

16.

Eine neue Vereinfachung leitet man aus folgender Bemerkung her. Da nach Artikel 14

$$\pm [r, R] \times [r, R^{\beta-1}] = [r, R^2] \times [r, R^{\beta-2}] = \pm [r, R^3]\,[r, R^{\beta-3}] = \cdots = n$$

ist, wo (im ersten, dritten, u. s. w. Producte) das obere oder untere Zeichen

zu nehmen ist, je nachdem $\frac{n-1}{\beta}$ gerade oder ungerade ist, so muss sein: im ersteren Falle:

$$\cos(f'+f^{(\beta-1)}) = \cos(f''+f^{(\beta-2)}) = \quad \cos(f'''+f^{(\beta-3)}) = \cdots = 1,$$

im letzteren Falle:

$$-\cos(f'+f^{(\beta-1)}) = \cos(f''+f^{(\beta-2)}) = -\cos(f'''+f^{(\beta-3)}) = \cdots = 1,$$

und in beiden Fällen:

$$\sin(f'+f^{(\beta-1)}) = \sin(f''+f^{(\beta-2)}) = \quad \sin(f'''+f^{(\beta-3)}) = \cdots = 0.$$

Daher kann man setzen:

im ersteren Falle: $f^{(\beta-1)} = \quad -f',\ f^{(\beta-2)} = \quad -f'',\ f^{(\beta-3)} = \quad -f''',\ldots$
im letzteren Falle: $f^{(\beta-1)} = 180^\circ - f',\ f^{(\beta-2)} = 180^\circ - f'',\ f^{(\beta-3)} = 180^\circ - f''',\ldots$

Hieraus aber folgt, dass

im ersteren Falle

$$b^{(\beta-2)} = b',\quad b^{(\beta-3)} = b'',\quad b^{(\beta-4)} = b''',\ \cdots,$$
$$A^{(\beta-2)} = A',\ A^{(\beta-3)} = A'',\ A^{(\beta-4)} = A''',\ \cdots,$$

im letzteren Falle aber

$$b^{(\beta-2)} = b' - 180^\circ,\quad b^{(\beta-3)} = b'' + 180^\circ,\quad b^{(\beta-4)} = b''' - 180^\circ,\ \cdots$$
$$A^{(\beta-2)} = -A',\qquad A^{(\beta-3)} = -A'',\qquad A^{(\beta-4)} = -A''',\ \cdots$$

ist, so dass die Anzahl der Functionen $A', A'', A''', \ldots$ sich auf die Hälfte reduciert. Hieraus folgt ferner, dass

im ersteren Falle:

$$f' = \frac{1}{\beta}\left(2b' + 2b'' + \cdots + 2b^{(\frac{1}{2}\beta-1)}\right)$$

$$\left(\frac{n-1}{\beta},\ 1\right) = -\frac{1}{\beta} + \frac{\sqrt{n}}{\beta}\Big\{2\cos f' + 2\cos(2f'-b') + 2\cos(3f'-b'-b'') + \cdots$$
$$+ 2\cos\left((\tfrac{1}{2}\beta-1)f' - b' - b'' - \cdots - b^{(\frac{1}{2}\beta-2)}\right) + \cos(\tfrac{1}{2}\beta f' - b' - b'' - \cdots - b^{(\frac{1}{2}\beta-1)}\Big\},$$

(wo das letzte Glied offenbar $= \cos 0 = 1$ ist), oder

$$f' = \frac{1}{\beta}\left(2b' + 2b'' + \cdots + 2b^{(\frac{1}{2}(\beta-3))} + b^{(\frac{1}{2}(\beta-1))}\right)$$

$$\left(\frac{n-1}{\beta},\ 1\right) = -\frac{1}{\beta} + \frac{\sqrt{n}}{\beta}\Big\{2\cos f' + 2\cos(2f'-b') + 2\cos(3f'-b'-b'') + \cdots$$
$$+ 2\cos\left(\tfrac{1}{2}(\beta-1)f' - b' - b'' - \cdots - b^{(\frac{1}{2}(\beta-3))}\right)\Big\}$$

ist, je nachdem β gerade oder ungerade ist, und

im letzteren Falle:

$$f' = \frac{1}{\beta}(2b' + 2b'' + \cdots + 2b^{(\frac{1}{2}\beta - 1)})$$

$$\left(\frac{n-1}{\beta}, 1\right) = -\frac{1}{\beta} + \frac{\sqrt{n}}{\beta}\Big\{2\cos(2f' - b') + 2\cos(4f' - b' - b'' - b''') + \cdots$$
$$+ 2\cos\left((\tfrac{1}{2}\beta - 2)f' - b' - b'' - \cdots - b^{(\frac{1}{2}\beta - 3)}\right) + \cos(\tfrac{1}{2}\beta f' - b' - b'' - \cdots - b^{(\frac{1}{2}\beta - 1)})\Big\}$$
$$+ i\frac{\sqrt{n}}{\beta}\Big\{2\sin f' + 2\sin(3f' - b' - b'') + \cdots + 2\sin\left((\tfrac{1}{2}\beta - 1)f' - b' - b'' - \cdots\right.$$
$$\left. - b^{(\frac{1}{2}\beta - 2)}\right)\Big\}$$

oder

$$f' = \frac{1}{\beta}(2b' + 2b'' + \cdots + 2b^{(\frac{1}{2}\beta - 1)} + 180^\circ)$$

$$\left(\frac{n-1}{\beta}, 1\right) = -\frac{1}{\beta} + \frac{\sqrt{n}}{\beta}\Big\{2\cos(2f' - b') + 2\cos(4f' - b' - b'' - b''') + \cdots$$
$$+ 2\cos\left((\tfrac{1}{2}\beta - 1)f' - b' - b'' - \cdots - b^{(\frac{1}{2}\beta - 2)}\right)\Big\}$$
$$+ i\frac{\sqrt{n}}{\beta}\Big\{2\sin f' + 2\sin(3f' - b' - b'') + \cdots + 2\sin\left((\tfrac{1}{2}\beta - 2)f' - b' - b'' - \cdots\right.$$
$$\left. - b^{(\frac{1}{2}\beta - 3)}\right) + \sin\left((\tfrac{1}{2}\beta - 1)f' - b' - b'' - \cdots - b^{(\frac{1}{2}\beta - 2)}\right)\Big\},$$

je nachdem $\frac{1}{2}\beta$ gerade oder ungerade ist. Von den übrigen Perioden von $\frac{n-1}{\beta}$ Gliedern gilt dasselbe, was wir oben angemerkt haben. Allgemein schliesst man also hieraus, dass zur Bestimmung dieser Perioden die Teilung des ganzen Kreises in β Teile, von welcher die Construction der Winkel $b', b'', b''', \ldots$ rational abhängt, ferner die Teilung des Winkels $b' + b'' + b''' + \ldots$ in β Teile, endlich die Ausziehung der Quadratwurzel $\sqrt{n}$ erforderlich ist. Wenn nun sogleich $\beta = \frac{1}{2}(n-1)$ gesetzt wird, so fallen jene Perioden offenbar mit den doppelten Cosinus der Winkel $\frac{360^\circ}{n}$, $2\frac{360^\circ}{n}$, $3\frac{360^\circ}{n}$, $\ldots$, $\frac{1}{2}(n-1)\frac{360^\circ}{n}$ zusammen, so dass die Teilung des Kreises in n Teile abhängt von der Teilung des ganzen Kreises in $\frac{1}{2}(n-1)$ Teile, von der Teilung eines Winkels, welcher nach Ausführung jener Teilung construiert werden kann, in $\frac{1}{2}(n-1)$ Teile und von der Wurzelgrösse $\sqrt{n}$. Wenn man bis zu dem Sinus der Winkel $\frac{360^\circ}{n}$, ... fortgehen soll, so ist noch eine Operation mehr erforderlich.

17.

Wir nehmen zur besseren Erläuterung das **Beispiel** des Artikels 13 wieder auf, wo wir fanden:

$$A' = A''' = 2 + 4R + R^3 + 2R^4 = 2R - 2R^2 - R^3$$
$$A'' = 2 + R + 4R^2 + 2R^3 = - R + 2R^2 - 2R^4.$$

Nimmt man für R den Wert $\cos 72° + i \sin 72°$, so ist:

$$A' = A''' = 2 \cos 72° - 3 \cos 144° + i(2 \sin 72° - \sin 144°)$$
$$A'' = - 3 \cos 72° + 2 \cos 144° + i(\sin 72° + 2 \sin 144°).$$

Es werden daher die Winkel b', b'', ... durch die Gleichungen bestimmt werden:

1) $$\sin b' = \frac{2 \sin 72° - \sin 144°}{\sqrt{11}}$$

2) $$\cos b' = \frac{2 \cos 72° - 3 \cos 144°}{\sqrt{11}}$$

3) $$\operatorname{tang} b' = \frac{2 \sin 72° - \sin 144°}{2 \cos 72° - 3 \cos 144°}$$

4) $$\sin b'' = \frac{\sin 72° + 2 \sin 144°}{\sqrt{11}}$$

5) $$\cos b'' = \frac{-3 \cos 72° + 2 \cos 144°}{\sqrt{11}}$$

6) $$\operatorname{tang} b'' = \frac{\sin 72° + 2 \sin 144°}{-3 \cos 72° + 2 \cos 144°}.$$

Jede der Gleichungen 1, 2, 3 genügt zur Bestimmung des Winkels b', wenn der Quadrant, in welchem er zu nehmen ist, bekannt ist; dieser wird aus den Vorzeichen der Grössen $2 \sin 72° - \sin 144°$, $2 \cos 72° - 3 \cos 144°$ entschieden werden müssen; dasselbe gilt vom Winkel b''.

In unserm Falle wird b' zwischen 0 und 90°, b'' zwischen 90° und 180° genommen werden. Wenn Zähler und Nenner der Gleichung 3) mit $-3 \cos 72° + 2 \cos 144°$ multipliciert werden, so geht sie über in die folgende:

$$\operatorname{tang} b' = \frac{2}{31}\{- \sin 72° + 13 \sin 144°\}$$

und ebenso geht aus Gleichung 6), wenn Zähler und Nenner mit $2 \cos 72° - 3 \cos 144°$ multipliciert werden, die folgende Gleichung hervor:

$$\operatorname{tang} b'' = \frac{2}{31}\{- 13 \sin 72° - \sin 144°\}.$$

Hieraus ergeben sich die numerischen Werte:

tang $b' = +0,4316226944$, logtang $b' = 9,6351042715$, $b' = 23°20'46''.04603$
tang $b'' = -0,8355819332$, logtang $b'' = 9,9219890411n$, $b'' = 140°\ 7'\ 6''.52441$,

woraus folgt:

$$5f' = 186°48'38''.\ 61647, \quad f' = 37°21'43''.\ 723294.$$

Wir erhalten daher:

$$(2,1) = -\frac{1}{5} + \frac{\sqrt{11}}{5}\{2\cos 37°21'43''.\ 723294 + 2\cos 51°22'41''.\ 400558\}$$

$$(2,2) = -\frac{1}{5} + \frac{\sqrt{11}}{5}\{2\cos 325°21'43''.\ 723294 + 2\cos 267°22'41''.\ 400558\}$$

$$(2,4) = -\frac{1}{5} + \frac{\sqrt{11}}{5}\{2\cos 253°21'43''.\ 723294 + 2\cos 123°22'41''.\ 400558\}$$

$$(2,8) = -\frac{1}{5} + \frac{\sqrt{11}}{5}\{2\cos 181°21'43''.\ 723294 + 2\cos 339°22'41''.\ 400558\}$$

$$(2,5) = -\frac{1}{5} + \frac{\sqrt{11}}{5}\{2\cos 109°21'43''.\ 723294 + 2\cos 195°22'41''.\ 400558\},$$

und hieraus findet man:

$$(2,1) = +1,6825070652 = 2\cos\frac{360°}{11}$$

$$(2,2) = +0,8308299 = 2\cos\frac{720°}{11}$$

$$(2,4) = \quad = 2\cos\frac{1440°}{11}$$

$$(2,8) = \quad = 2\cos\frac{2880°}{11}$$

$$(2,5) = \quad = 2\cos\frac{1800°}{11}.$$

18.

Ein anderes **Beispiel** liefert uns die Gleichung $x^{17} - 1 = 0$, die wir nach einer andern Methode schon in den *„Arithmetischen Untersuchungen“* behandelt haben. Wir setzen also $n = 17$, $\beta = 8$, $g = 3$. Daher entsprechen

den Zahlen:	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16
die Indices:	0.	14.	1.	12.	5.	15.	11.	10.	2.	3.	7.	13.	4.	9.	6.	8.

Hieraus finden wir:

$$A' = A'''''' = * + 2R + 2R^2 + * + 3R^4 + 4R^5 + 2R^6 + 2R^7$$
$$A'' = A''''' = 2 + 3R + * + R^3 + R^4 + 3R^5 + 4R^6 + R^7$$
$$A''' = A'''' = 3 + 3R + 2R^2 + 3R^3 + * + R^5 + 2R^6 + R^7$$

oder, da in diesem Falle $R^4 + 1 = 0$ ist:

$$A' = A'''''' = -3 - 2R - 2R^3$$
$$A'' = A''''' = 1 - 4R^2$$
$$A''' = A'''' = 3 + 2R + 2R^3.$$

Setzt man daher $R = \cos 45° + i \sin 45°$, so wird:

$$A' = A'''''' = -3 - 2i\sqrt{2}, \quad A'' = A''''' = 1 - 4i, \quad A''' = A'''' = 3 + 2i\sqrt{2}.$$

Man findet daher die Grössen b', b'', b''' durch die Gleichungen:

$$\sin b' = -\sqrt{\frac{8}{17}}, \ \sin b'' = -\sqrt{\frac{16}{17}}, \ \sin b''' = +\sqrt{\frac{8}{17}}$$
$$\cos b' = -\sqrt{\frac{9}{17}}, \ \cos b'' = +\sqrt{\frac{1}{17}}, \ \cos b''' = +\sqrt{\frac{9}{17}}$$
$$\operatorname{tang} b' = +\sqrt{\frac{8}{9}}, \ \operatorname{tang} b'' = -4, \quad \operatorname{tang} b''' = +\sqrt{\frac{8}{9}},$$

und aus diesen ergiebt sich:

$$b' = 223°18'49'', \ b'' = 284°2'10'', \ b''' = 43°18'49'' = b' - 180°.$$
$$4f' = 550°39'48'', \ f' = 137°39'57''.$$

$$(2,\ 1) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 137°39'57'' + 2\cos 52°1'5'' + 2\cos 265°38'52'' + 1\}$$

$$(2,\ 3) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 92°39'57'' + 2\cos 322°1'5'' + 2\cos 130°38'52'' - 1\}$$

$$(2,\ 9) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 47°39'57'' + 2\cos 232°1'5'' + 2\cos 355°38'52'' + 1\}$$

$$(2, 10) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 2°39'57'' + 2\cos 142°1'5'' + 2\cos 220°38'52'' - 1\}$$

$$(2, 13) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 317°39'57'' + 2\cos 52°1'5'' + 2\cos 85°38'52'' + 1\}$$

$$(2,\ 5) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 272°39'57'' + 2\cos 322°1'5'' + 2\cos 310°38'52'' - 1\}$$

$$(2, 15) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 227°39'57'' + 2\cos 232°1'5'' + 2\cos 175°38'52'' + 1\}$$

$$(2, 11) = -\frac{1}{8} + \frac{\sqrt{17}}{8}\{2\cos 182°39'57'' + 2\cos 142°1'5'' + 2\cos 40°38'52'' - 1\}$$

$$\frac{1}{2}(2,\ 1) = +0{,}092268 = \cos\frac{4}{17}360°$$
$$\frac{1}{2}(2,\ 3) = \qquad = \cos\frac{5}{17}360°$$
$$\frac{1}{2}(2,\ 9) = \qquad = \cos\frac{2}{17}360°$$
$$\frac{1}{2}(2, 10) = \qquad = \cos\frac{6}{17}360°$$
$$\frac{1}{2}(2, 13) = +0{,}93247 \quad = \cos\frac{1}{17}360°$$
$$\frac{1}{2}(2,\ 5) = \qquad = \cos\frac{3}{17}360°$$
$$\frac{1}{2}(2, 15) = \qquad = \cos\frac{8}{17}360°$$
$$\frac{1}{2}(2, 11) = \qquad = \cos\frac{7}{17}360°.$$

* * *

Von diesen allgemeineren Untersuchungen über die Functionen $[r, R]$, welche die zweite in den *„Arithmetischen Untersuchungen“* Artikel 360 (vgl. oben S. 434) begonnene Theorie der reinen Gleichungen in helleres Licht setzen und erweitern, gehen wir zur genaueren Betrachtung gewisser specieller Fälle über (wenn nämlich für β bestimmte Werte genommen werden); es ergeben sich hieraus mehrere nicht minder fruchtbare wie elegante Erörterungen, von denen einige allerdings schon in den *„Arithmetischen Untersuchungen“*, aber nach einer anderen Methode behandelt worden, andere aber als völlig neu zu betrachten sind. Die Entwicklung des wunderbaren Zusammenhanges aber zwischen diesen Untersuchungen und der höheren Arithmetik, welche dadurch sehr bedeutende und bisher unvermutete Erweiterungen erfahren hat, behalten wir uns für eine demnächst zu veröffentlichende Abhandlung vor. — Übrigens werden wir in der ganzen folgenden Untersuchung annehmen, dass für r eine eigentliche Wurzel der Gleichung $x^n - 1 = 0$ und für R eine eigentliche Wurzel der Gleichung $R^\beta - 1 = 0$ genommen wird.

19.

Wir beginnen mit dem Werte $\beta = 2$, wo also für R der Wert -1 zu nehmen ist. Unsere Function $[r, R]$ wird daher:

$$= r - r^g + r^{g^2} - r^{g^3} + \cdots - r^{g^{n-2}}$$

und man hat:

$$[r, R] = -[r^g, R] = +[r^{g^2}, R] = -[r^{g^3}, R] = \cdots$$

und allgemein, wenn λ eine beliebige durch n nicht teilbare ganze Zahl bezeichnet:

$$[r^\lambda, R] = +[r, R], \text{ wenn } \lambda \text{ quadratischer Rest von } n$$
$$[r^\lambda, R] = -[r, R], \text{ wenn } \lambda \text{ quadratischer Nichtrest von } n \text{ ist.}$$

Ferner werden offenbar, wenn die unter den Zahlen $1, 2, 3, \ldots, n-1$ enthaltenen quadratischen Reste von n unbestimmt mit a und die Nichtreste von n innerhalb desselben Intervalls mit b bezeichnet werden, die Zahlen

$$1, g^2, g^4, \ldots, g^{n-3},$$

wenn man auf die Reihenfolge keine Rücksicht nimmt, nach dem Modul n den Zahlen a und ebenso die Zahlen

$$g, g^3, g^5, \ldots, g^{n-2}$$

den Zahlen b congruent sein, so dass $[r, R] = \Sigma r^a - \Sigma r^b$ wird.

Wenn wir daher $\frac{360^\circ}{n} = \omega$ und $r = \cos k\omega + i \sin k\omega$ setzen, so wird:

$$[r, R] = \Sigma \cos ak\omega - \Sigma \cos bk\omega + i\Sigma \sin ak\omega - i\Sigma \sin bk\omega.$$

Nun ist nach Artikel 14 das Quadrat der Function $[r, R]$ gleich $+n$ oder gleich $-n$, je nachdem n von der Form $4z+1$ oder $4z-1$ ist, und daher ist in dem ersteren Falle $[r, R] = \pm\sqrt{n}$, in dem letzteren $[r, R] = \pm i\sqrt{n}$, das der Wurzelgrösse vorgesetzte Vorzeichen aber bleibt zweifelhaft. Hieraus ergeben sich die folgenden Summationen:

I. Wenn n von der Form $4z+1$ ist:

$$\Sigma \cos ak\omega - \Sigma \cos bk\omega = \pm\sqrt{n}$$
$$\Sigma \sin ak\omega - \Sigma \sin bk\omega = 0.$$

II. Wenn n von der Form $4z-1$ ist:

$$\Sigma \cos ak\omega - \Sigma \cos bk\omega = 0$$
$$\Sigma \sin ak\omega - \Sigma \sin bk\omega = \pm\sqrt{n}.$$

Ferner wird, da offenbar der ganze Complex der Zahlen a, b mit den Zahlen $1, 2, 3, \ldots, n-1$ übereinstimmt,

$$\Sigma r^a + \Sigma r^b = r + r^2 + r^3 + \cdots + r^{n-1} = -1.$$

und somit:

$$\Sigma \cos ak\omega + \Sigma \cos bk\omega = -1$$
$$\Sigma \sin ak\omega + \Sigma \sin bk\omega = 0.$$

Hiernach ergeben sich aus den vorigen Summationen die folgenden:

I. Für den ersten Fall:

$$\Sigma \cos ak\omega = -\tfrac{1}{2} \pm \tfrac{1}{2} \sqrt{n}$$
$$\Sigma \cos bk\omega = -\tfrac{1}{2} \mp \tfrac{1}{2} \sqrt{n}$$
$$\Sigma \sin ak\omega = \Sigma \sin bk\omega = 0.$$

II. Für den zweiten Fall:

$$\Sigma \cos ak\omega = \Sigma \cos bk\omega = -\tfrac{1}{2}$$
$$\Sigma \sin ak\omega = \pm \tfrac{1}{2} \sqrt{n}$$
$$\Sigma \sin bk\omega = \mp \tfrac{1}{2} \sqrt{n}.$$

Diese Summationen sind nach einer nicht sehr verschiedenen Methode schon in den „*Arithmetischen Untersuchungen*“ Artikel 356 (vgl. oben S. 425) ermittelt worden; zwar vermag keine von beiden Methoden die Zweideutigkeit des der Wurzelgrösse vorzusetzenden Zeichens zu beseitigen, doch haben wir diese Lücke neulich in einer besonderen Abhandlung ausgefüllt, wo wir bewiesen haben, dass für $k = 1$ in allen angegebenen Formeln die oberen Vorzeichen genommen werden müssen.

Beweis einiger Sätze über die Perioden der Klassen der binären Formen zweiten Grades.



Satz I. Die Anzahl der (eigentlich primitiven) Klassen mit derselben Determinante, welche zur P^{ten} Potenz erhoben, wo P entweder eine Primzahl oder die Potenz einer Primzahl gleich p^π ist, die Hauptklasse K hervorbringen, ist entweder gleich 1 oder gleich einer Potenz derselben Primzahl p.

Beweis. Es sei (Ω) die vollständige Gruppe aller in Rede stehenden Klassen und n ihre Anzahl. Da die Hauptklasse K notwendig in (Ω) enthalten ist, so ist der Satz evident, wenn sie allein darin vorkommt. Kommen aber noch andere darin vor, so wird die Anzahl der in der Periode einer jeden enthaltenen Klassen eine Potenz von p sein. Es sei A eine von ihnen und es werde vorausgesetzt, dass ihre Periode $(\mathfrak{A})$ p^α Klassen enthalte, welche alle in (Ω) enthalten sein werden. Wenn nun die Klassen dieser Periode $(\mathfrak{A})$ den Complex (Ω) erschöpfen, so hat man $p^\alpha = n$, und der Satz wird bewiesen sein; wenn nicht, so sei B eine beliebige nicht in $(\mathfrak{A})$ enthaltene Klasse von (Ω), und man nehme an, dass ihre Periode entwickelt sei, bis man zu einer Klasse bB gelangt, welche gleichzeitig unter den Klassen von $(\mathfrak{A})$ vorkommt, was notwendig eintreten muss, da wenigstens die Hauptklasse dieser Periode und der Periode $(\mathfrak{A})$ gemeinschaftlich ist. Setzt man nun voraus, dass bB die erste Klasse in der Periode B ist, welche auch in $(\mathfrak{A})$ vorkommt, oder dass b so klein wie möglich ist, so behaupte ich:

1. dass b eine Potenz von p ist. Denn es ist klar, dass man, wenn man $b = p^\beta h$, $bB = iA$ und $hk \equiv 1$ (mod. p^π) setzt (was möglich ist), $kbB = p^\beta hkB = p^\beta B = ikA$ hat, d. h. dass $p^\beta B$ auch unter den Klassen von $(\mathfrak{A})$ sich findet, woraus folgt, dass $h = 1$ und $b = p^\beta$ ist.

2. dass, wenn man die Klassen $K, B, 2B, \ldots, (b-1)B$ mit $(\mathfrak{B})$ bezeichnet, alle Compositionen einer Klasse von $(\mathfrak{A})$ mit einer Klasse von $(\mathfrak{B})$ $p^{\alpha+\beta}$ verschiedene Klassen geben werden. Denn nimmt man $mA + nB = m'A + n'B$ und $n = n'$ an, so hat man notwendig $m = m'$; ist $n > n'$, so hat man $(n - n')B = (m' - m)A$, was unmöglich ist, wenn man nicht $n = n'$ hat.

3. dass diese $p^{\alpha+\beta}$ verschiedenen Klassen unter (Ω) enthalten sind, was evident ist.

Wenn nun diese $p^{\alpha+\beta}$ Klassen den Complex (Ω) erschöpfen, so ist der Satz bewiesen; wenn nicht, so wähle man eine andere unter jenen nicht enthaltene Klasse von (Ω) aus, etwa C, und setze ihre Periode fort, bis man zu einer Klasse gelangt, welche bereits unter den aus $(\mathfrak{A})$ und $(\mathfrak{B})$ zusammengesetzten Klassen enthalten ist. Durch eine der vorigen ähnliche Schlussreihe zeigt man, dass der Exponent dieser Klasse eine Potenz von p sein muss, $= p^\gamma$, und dass die Composition der p^γ ersten Klassen der Periode von C mit den $p^{\alpha+\beta}$ bereits gefundenen Klassen $p^{\alpha+\beta+\gamma}$ verschiedene Klassen giebt, welche alle unter (Ω) enthalten sind. Wenn diese Klassen noch nicht (Ω) erschöpfen, so behandle man in derselben Weise eine vierte Klasse D u. s. w. und es ist klar, da (Ω) aus einer endlichen Anzahl von Klassen besteht, dass diese Operationen ebenfalls aufhören werden und dass n gleich einer Potenz von p wird.

Satz II. Wenn die Anzahl aller Klassen des Hauptgeschlechts durch $a^\alpha b^\beta c^\gamma \ldots$ ausgedrückt wird, wo $a, b, c \ldots$ verschiedene Primzahlen bezeichnen, so giebt es in diesem Geschlechte $a^\alpha, b^\beta, c^\gamma, \ldots$ Klassen, welche, zur Potenz $a^\alpha, b^\beta, c^\gamma, \ldots$ respective erhoben, die Hauptklasse hervorbringen.

Beweis. Sind $A, A', A'', \ldots$ sämtliche Klassen, welche zur Potenz a^β erhoben die Hauptklasse K hervorbringen und ist $(\mathfrak{A})$ der Complex derselben, haben ferner $B, B', B'', \ldots, (\mathfrak{B})$, sowie $C, C', C'', \ldots, (\mathfrak{C})$ u. s. w. analoge Bedeutungen, so behaupte ich, dass aus der Composition aller Klassen von $(\mathfrak{A})$ mit allen Klassen von $(\mathfrak{B})$ mit allen Klassen von $(\mathfrak{C})$ u. s. w. unter einander verschiedene Klassen hervorgehen. Denn wenn $A + B + C + \ldots = A' + B' + C' + \ldots$ ist, so hat man, wenn man $A - A' = A''$, $B - B' = B''$, u. s. w. setzt:

$$A'' + B'' + C'' + \cdots = K,$$

mithin, wenn man zur Potenz $b^\beta c^\gamma \ldots$ erhebt, $(b^\beta c^\gamma \ldots) A'' = K$, woraus sich leicht ergiebt $A'' = K$ und $A = A'$ und auf dieselbe Weise hat man: $B = B'$, $C = C'$, u. s. w. Die Gesamtheit dieser Klassen sei gleich (S). Ferner ist klar, dass alle diese Klassen zum Hauptgeschlechte gehören. Endlich kann es keine Klasse in dem Hauptgeschlechte geben, die nicht unter (S) enthalten wäre. Es sei ...

Über den Zusammenhang zwischen der Anzahl der Klassen, in welche die binären Formen zweiten Grades zerfallen, und ihrer Determinante.

I.

1.

Es sind schon dreiunddreissig Jahre verflossen, seit ich die Prinzipien des wunderbaren Zusammenhanges, welchem die vorliegende Abhandlung gewidmet ist, entdeckte, wie ich schon am Schlusse der „*Arithmetischen Untersuchungen*“ bemerkt habe. Aber andere Beschäftigungen zogen mich lange Zeit hindurch von dieser Untersuchung ab, bis ich in neuerer Zeit wieder zu ihr zurückzukehren und durch erneute Bemühungen sie zu erweitern vermochte. Da jedoch dieser neue Teil der höheren Arithmetik die Grenzen einer Abhandlung überschreitet, so soll diese erste Abhandlung den Formen mit negativer Determinante gewidmet sein; die Formen mit positiver Determinante aber, welche eine ganz eigentümliche Behandlung erfordern, müssen einer andern Abhandlung vorbehalten bleiben.

2.

Die Grundlage des ganzen Gegenstandes bildet eine eigentümliche Untersuchung über die Anzahl aller Combinationen der ganzzahligen Werte, welche zwei unbestimmte ganze Zahlen innerhalb eines vorgeschriebenen Gebietes annehmen. Offenbar kann diese Aufgabe auch unter geometrischer Fassung dargestellt werden, nämlich die Anzahl der complexen Zahlen zu ermitteln, deren Darstellung innerhalb einer vorgeschriebenen Figur fällt. Die Beschaffenheit der Figur wird von der Beschaffenheit der sie umgebenden Linie und somit entweder von einer einzigen Gleichung zwischen den Coordinaten x, y (wenn der Umfang eine in sich zurückkehrende Kurve ist) oder von mehreren solchen Gleichungen (wenn er aus mehreren

gekrümmten oder geraden Teilen besteht) abhängen, und es wird unserm Belieben überlassen sein, ob wir die den complexen ganzen Zahlen entsprechenden Punkte, welche etwa auf dem Umfange gelegen sind, der Anzahl zuzählen, oder von ihr ausschliessen wollen.

Bei der analytischen Darstellung jener Aufgabe können jene Grenzbedingungen immer so ausgedrückt werden, dass entweder eine oder mehrere gegebene Functionen $P, Q, R, \ldots$ der Veränderlichen x, y positive oder nichtnegative (je nachdem der Wert 0 ausgeschlossen oder zugelassen wird) Werte erhalten sollen.

So ist z. B., wenn die vorgeschriebene Figur ein Kreis ist, dessen Radius $= \sqrt{A}$ ist, während sein Mittelpunkt in einen einer ganzen complexen Zahl entsprechenden Punkt fällt, die analytische Bedingung die, dass $A - x^2 - y^2$ nicht negativ sei, wofern wir, was wir immer annehmen werden, die Punkte, welche auf der Peripherie selbst liegen, beibehalten wollen. Ist die Figur ein Dreieck, so müssen die drei linearen Functionen $ax + by + c$, $a'x + b'y + c'$, $a''x + b''y + c''$ nichtnegative Werte haben, und ähnlich in andern Fällen.

3.

Eine exacte Lösung der Aufgabe muss, allgemein zu reden, in der Weise vorgehen, dass zunächst aus der Natur der Bedingungen die eine Veränderliche z. B. x in Grenzen eingeschlossen werden muss, innerhalb deren die einzelnen ganzen Werte der Reihe nach verlaufen, und ermittelt werden muss, wieviele ganzzahligen Werte der andern Veränderlichen y jedem einzelnen Werte von x entsprechen; die Anzahlen dieser müssen sodann zu einer Summe vereinigt werden. In speciellen Fällen giebt es meistenteils specielle Kunstgriffe zur Abkürzung der Arbeit.

Ist z. B. die Figur wie oben ein Kreis mit dem Radius $\sqrt{A}$, so sei r die grösste unterhalb $\sqrt{A}$ liegende ganze Zahl oder $\sqrt{A}$ selbst, wenn A ein Quadrat ist. Ebenso seien $r', r'', r''', \ldots, r^{(r)}$ die grössten unterhalb $\sqrt{A-1}$, $\sqrt{A-4}$, $\sqrt{A-9}, \ldots, \sqrt{A-r^2}$ respective liegenden ganzen Zahlen. Dann ist die gesuchte Anzahl:

$$= 2r + 1 + 2(2r' + 1) + 2(2r'' + 1) + 2(2r''' + 1) + \cdots$$
$$= 1 + 4r + 4r' + 4r'' + 4r''' + \cdots + 4r^{(r)}.$$

Kürzer ist in diesem Beispiel die folgende Methode. Es sei q die grösste unterhalb $\sqrt{\tfrac{1}{2}A}$ gelegene ganze Zahl (oder gleich $\sqrt{\tfrac{1}{2}A}$, sobald dieses eine ganze Zahl ist) und ebenso seien $r^{(q+1)}, r^{(q+2)}, r^{(q+3)}, \ldots$ die grössten unterhalb $\sqrt{A-(q+1)^2}$, $\sqrt{A-(q+2)^2}$, $\sqrt{A-(q+3)^2}, \ldots$, $\sqrt{A-r^2}$ gelegenen ganzen Zahlen. Dann ist die gesuchte Anzahl:

$$= 4q^2 + 1 + 4r + 8(r^{(q+1)} + r^{(q+2)} + r^{(q+3)} + \cdots + r^{(r)}).$$

Nach dieser Formel ist die Anzahl ermittelt worden:

A		A		A	
100	317	1 000	3 149	10 000	31 417
200	633	2 000	6 293	20 000	62 845
300	949	3 000	9 425	30 000	94 237
400	1257	4 000	12 581	40 000	125 629
500	1581	5 000	15 705	50 000	157 093
600	1885	6 000	18 853	60 000	188 453
700	2209	7 000	21 993	70 000	219 901
800	2521	8 000	25 137	80 000	251 305
900	2821	9 000	28 269	90 000	282 697
1000	3149	10 000	31 417	100 000	314 197.

4.

Für unsern Zweck ist eine genaue Bestimmung nicht erforderlich, vielmehr nur die Ermittlung eines Ausdrucks, welcher die genaue Anzahl in beliebiger Annäherung ergiebt, sobald man die Grenzen ins Unendliche erweitert. Vor allen Dingen müssen wir aber, da dies etwas willkürliches enthält, die Sache genauer entwickeln.

Wir nehmen also an, dass die Functionen P, Q, R, ... ausser den Veränderlichen x, y ein konstantes Element k enthalten, so dass die einzelnen Functionen P, Q, R, ... homogene Functionen der drei Grössen x, y, k sind. Auf diese Weise wird die durch die Gleichung $P = 0$, $Q = 0$, $R = 0$, ... bestimmte Figur von k abhängen derart, dass verschiedenen Werten von k ähnliche und mit Bezug auf den Coordinatenanfangspunkt ähnlich gelegene Figuren entsprechen, und die analogen linearen Dimensionen werden den Werten von k, die Flächeninhalte aber den Werten von k^2 proportional sein. Bezeichnet man nun die Anzahl der Punkte innerhalb der Figur mit M, den Flächeninhalt mit V, so müssen offenbar mit wachsendem k auch M und V wachsen; wächst aber k ins Unendliche, so werden sich M und V beliebig weit dem Verhältnis der Gleichheit nähern, oder, wenn man elementare Klarheit wünscht, es wird, wenn eine beliebig kleine Grösse λ gegeben ist, immer eine solche Grenze angegeben werden können, dass für jeden diese Grenze übersteigenden Wert von k sicher $\frac{M}{V}$ zwischen $1 - \lambda$ und $1 + \lambda$ liegen muss. Nach der üblichen Ausdrucksweise kann man dies so andeuten: es werde $M = V$ für einen unendlichen Wert von k.

In unserem Beispiel findet die erforderliche Bedingung statt, wenn man $k = \sqrt{A}$ setzt, und es wird die Kurve ein Kreis, dessen Flächeninhalt $= \pi A$ ist, wo π den halben Umfang eines Kreises mit dem Radius 1 bezeichnet. Die oben angegebenen Zahlen lassen die Convergenz deutlich erkennen.

Wenn es sich übrigens der Mühe lohnte, würden wir den Beweis dieses Satzes in aller Strenge führen können; indessen unterdrücken wir denselben an dieser Stelle lieber und gehen zu schwierigeren Sachen über.

5.

In dieser Abhandlung wird die Grenze durch eine einzige Gleichung von der Form $ax^2+2bxy+cy^2=A$ dargestellt, wo a, b, c ganze Zahlen sind und b^2-ac eine negative Zahl ist, die wir gleich $-D$ setzen. Offenbar wird die die Figur bestimmende Kurve eine Ellipse, und es ergiebt sich leicht, dass die Quadrate der Halbachsen die Wurzeln der Gleichung

$$(ac-b^2)q^2-A(a+c)q+A^2=0, \text{ oder gleich } A\cdot\frac{a+c\pm\sqrt{4b^2+(a-c)^2}}{2(ac-b^2)}$$

sind. Das Product dieser Wurzeln wird $\frac{A^2}{ac-b^2}=\frac{A^2}{D}$, somit die Fläche der Ellipse $=\frac{\pi A}{\sqrt{D}}$.

Hieraus folgt also, dass die Anzahl aller Combinationen von ganzzahligen Werten der Veränderlichen x, y, für welche der Ausdruck $ax^2+2bxy+cy^2$ den Wert A nicht übersteigt, mit wachsendem A sich beständig mehr der Grösse $\frac{\pi A}{\sqrt{D}}$ nähert und für ein unendlich grosses A diesem Werte gleichgesetzt werden muss. Ferner ist klar, dass es in dieser Hinsicht gleichgültig ist, ob die Combination $x=0$, $y=0$ den übrigen zugezählt oder davon ausgeschlossen wird. Auf diese Weise ist also die gesuchte Anzahl (im letzteren Sinne) nichts anderes, als das Aggregat der Anzahl der Darstellungen der einzelnen Zahlen $1, 2, 3, \ldots, A$ durch die binäre Form zweiten Grades $ax^2+2bxy+cy^2$, und da von jenen Zahlen die einen überhaupt nicht durch diese Form dargestellt werden können, die andern mehr oder weniger Darstellungen besitzen, so ist die Grösse $\frac{\pi}{\sqrt{D}}$ als mittlerer Wert der Anzahl der Darstellungen einer unbestimmten positiven Zahl durch irgend eine Form, deren Determinante gleich $-D$ ist, zu betrachten.

6.

Bevor wir zu einer allgemeinen Darlegung des Folgenden übergehen, schien es uns gut, einige besondere Fälle zu entwickeln, damit man die Art und Weise der Argumentation leichter durchdringen könne. Wir nehmen daher zunächst die Form x^2+y^2 wieder auf, für welche somit die Anzahl der Darstellungen einer unbestimmten Zahl den mittleren Wert π erhält. Die Anzahl der wirklichen Darstellungen einer gegebenen Zahl aber wird ohne Schwierigkeit aus den in den „*Arithmetischen Untersuchungen*“ begründeten allgemeinen Prinzipien bestimmt. Bezeichnen wir mit $f(A)$ die Anzahl der Darstellungen der Zahl A, so ist dieselbe gleich 4, wenn $A=1$ oder $=2$ oder eine Potenz von 2 ist; gleich

8, wenn A eine Primzahl von der Form $4n+1$ oder das Product einer solchen Primzahl in eine Potenz von 2 ist; gleich 0, wenn A eine Primzahl von der Form $4n+3$ oder durch eine solche Primzahl, aber nicht durch das Quadrat derselben, teilbar ist; endlich allgemein

$$\begin{aligned}\text{entweder } &= 4(\alpha+1)(\beta+1)(\gamma+1)\ldots\\ \text{oder } &= 0,\end{aligned}$$

je nachdem, sobald die Zahl A auf die Form $2^{\mu} S a^{\alpha} b^{\beta} c^{\gamma}, \ldots$ gebracht ist, wo $a, b, c, \ldots$ ungleiche Primzahlen von der Form $4n+1$ bezeichnen, S aber das Product aus den Primzahlen von der Form $4n+3$ ist, wenn etwa solche unter den Factoren der Zahl A vorkommen, je nachdem also die Zahl S ein Quadrat ist oder nicht. Es ist also klar, dass $f(A)$ einzig und allein von der Art und Weise abhängt, in welcher die Primzahlen 3, 5, 7, 11, 13, ... unter den Factoren der Zahl A vorkommen, so dass man allgemein setzen muss

$$f(A) = 4(3)\cdot(5)\cdot(7)\cdot(11)\cdot(13)\ldots,$$

wenn wir voraussetzen, dass $(3), (5), (7), \ldots$ so genommen werden, dass, wenn p eine Primzahl bezeichnet,

erstens $(p) = 1$ ist, falls p in A nicht aufgeht,

zweitens $(p) = \alpha + 1$ ist, falls p von der Form $4n+1$ und p^{α} die höchste in A aufgehende Potenz ist,

drittens $(p) = 0$ ist, falls p von der Form $4n+3$ und der Exponent der höchsten in A aufgehenden Potenz von p ungerade ist, endlich

viertens $(p) = 1$ ist, falls p von der Form $4n+3$ und der Exponent der höchsten in A aufgehenden Potenz von p gerade ist.

Offenbar ist der erste Fall unter dem zweiten und vierten enthalten.

Auf diese Weise schreiten also die Glieder der Reihe $f(1)$, $f(2)$, $f(3)$, $f(4), \ldots$ höchst unregelmässig fort, obwohl, je grösser die Anzahl genommen wird, der mittlere Wert $= \pi$ um so genauer daraus entstehen muss. Das Aggregat $f(1) + f(2) + f(3) + \cdots + f(A)$ wollen wir mit $F(A)$ bezeichnen.

7.

Setzen wir nun allgemein $f(m) + f(3m) = f'(m)$, so sieht man leicht, dass

$$f'(A) = 4(5)\cdot(7)\cdot(11)\cdot(13)\cdots$$

wird, d. h. es wird $f'(A)$ von der Beziehung von A zu 3 unabhängig sein, so dass die Irregularität der Reihe $f'(1)$, $f'(2)$, $f'(3)$, $f'(4)$, $f'(5)$, $f'(6), \ldots$ nicht nur später anfangen, sondern auch viel geringer sein wird. Setzen wir ferner:

$$f'(1) + f'(2) + f'(3) + f'(4) + \cdots + f'(m) = F'(m),$$

so ist:

$$F'(3A) = F(3A) + f(3) + f(6) + f(9) + \cdots + f(3A) = F(3A) + F(A).$$

Hieraus folgt leicht, dass, wenn A ins Unendliche wächst,

$$F'(3A) = 4\pi A$$

gesetzt werden muss, oder dass der mittlere Wert der Glieder der Reihe $f'(1), f'(2), f'(3), f'(4), \ldots$

$$= \frac{4}{3}\pi$$

ist.

Setzt man allgemein: $-f'(m) + f'(5m) = f''(m)$, so wird in ähnlicher Weise:

$$f''(A) = 4(7)\cdot(11)\cdot(13)\cdots,$$

oder es fallen aus der neuen Reihe $f''(1), f''(2), \ldots$ die von der Relation zu 5 abhängenden Unregelmässigkeiten heraus. Und setzt man das Aggregat

$$f''(1) + f''(2) + f''(3) + \cdots + f''(m) = F''(m),$$

so wird:

$$F''(5m) = -F'(m) + F'(5m),$$

woraus folgt, dass, wenn m ins Unendliche wächst,

$$F''(5m) = \tfrac{4}{3}\pi\cdot 4m$$

gesetzt werden muss, oder dass der mittlere Wert der Glieder der Reihe gleich $\frac{4}{5}\cdot\frac{4}{3}\pi$ ist.

Wenn wir in derselben Weise weiter fortgehen, indem wir neue Reihen bilden, bis wir die Factoren (7), (11), (13), (17), ... nach einander fortgeschafft haben, so werden diese sich mehr und mehr der Unveränderlichkeit nähern und die mittleren Werte werden der Reihe nach die neuen Factoren $\frac{8}{7}, \frac{12}{11}, \frac{12}{13}, \frac{16}{17}, \frac{20}{19}, \ldots$ erhalten, wo die Nenner die Primzahlen in natürlicher Reihenfolge, die Zähler aber um eine Einheit grösser oder kleiner sind, je nachdem jene Primzahlen von der Form $4n-1$ oder $4n+1$ sind. Da nun, wenn dieser Process ins Unendliche fortgesetzt wird, der konstante Wert 4 dem mittleren Werte immer näher kommen muss, so erhalten wir:

$$4 = \pi\cdot\frac{4}{3}\cdot\frac{4}{5}\cdot\frac{8}{7}\cdot\frac{12}{11}\cdot\frac{12}{13}\cdots\cdot \text{ in inf.}$$

oder:

$$\pi = 4\cdot\frac{3}{3+1}\cdot\frac{5}{5-1}\cdot\frac{7}{7+1}\cdot\frac{11}{11+1}\cdot\frac{13}{13-1}\cdots\cdot$$

Werden die einzelnen Brüche in unendliche Reihen entwickelt:

$$\frac{3}{3+1} = 1 - \frac{1}{3} + \frac{1}{9} - \frac{1}{27} + \cdots$$

$$\frac{5}{5-1} = 1 + \frac{1}{5} + \frac{1}{25} + \frac{1}{125} + \cdots$$

$$\frac{7}{7+1} = 1 - \frac{1}{7} + \frac{1}{49} - \frac{1}{343} + \cdots$$

u. s. w.,

so entwickelt man das Product leicht in:

$$1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\frac{1}{9}-\frac{1}{11}+\frac{1}{13}-\cdots,$$

und die Summe dieser Reihe ist, wie allgemein bekannt, gleich $\frac{1}{4}\pi$. In der That ist auf umgekehrtem Wege schon längst hieraus die Gleichheit zwischen $\frac{1}{4}\pi$ und dem unendlichen Producte $\frac{4}{3}\cdot\frac{4}{5}\cdot\frac{8}{7}\cdots$ von Euler abgeleitet worden (*Introd. in analysin inf.* T. I, Cap. XV, § 285).

8.

An zweiter Stelle betrachten wir die Form x^2+2y^2, für welche die Anzahl der Darstellungen einer unbestimmten Zahl einen mittleren Wert gleich $\frac{\pi}{\sqrt{2}}$ haben wird. Bezeichnet man mit $f(A)$ die Anzahl der Darstellungen der gegebenen Zahl A durch jene Form, so ist dieselbe gleich 2 für $A=1$ oder $A=2$ oder wenn A eine Potenz von 2 ist; ferner ist $f(A)=4$, wenn A eine aus der Reihe der Primzahlen, deren quadratischer Rest -2 ist, oder der Primzahlen von der Form $8k+1$, $8k+3$, also $A=3, 11, 17, 19, 41, 43, \ldots$ ist; endlich ist $f(A)=0$, wenn A eine Primzahl ist, von welcher -2 quadratischer Nichtrest ist, nämlich eine Zahl aus der Reihe 5, 7, 13, 23, 29, 31, ... oder von der Form $8k+5$ oder $8k+7$ ist. Allgemein muss man setzen

$$\begin{array}{ll}\text{entweder} & f(A)=2(\alpha+1)(\beta+1)(\gamma+1)\cdots\\ \text{oder} & f(A)=0,\end{array}$$

je nachdem, wenn die Zahl A auf die Form $2^\mu Sa^\alpha b^\beta c^\gamma\ldots$ gebracht ist, wo $a, b, c, \ldots$ ungleiche Primzahlen von der Form $8k+1$, $8k+3$ bezeichnen, dagegen S das Product aus den übrigen Zahlen (von der Form $8k+5$, $8k+7$) ist, wenn solche unter den Factoren der Zahl A enthalten sind, je nachdem also S ein Quadrat ist oder nicht. Hierauf gehen wir durch ganz ähnliche Schlussfolgerungen wie im vorigen Artikel von der Reihe $f(1), f(2), f(3), f(4), f(5), \ldots$ oder $2, 2, 4, 2, 0, 2, \ldots$ nach und nach zu immer mehr konstant werdenden Reihen fort, deren mittlere Werte der Reihe nach $\frac{\pi}{\sqrt{2}}$, $\frac{\pi}{\sqrt{2}}\cdot\frac{2}{3}$, $\frac{\pi}{\sqrt{2}}\cdot\frac{2}{3}\cdot\frac{6}{5}$, $\frac{\pi}{\sqrt{2}}\cdot\frac{2}{3}\cdot\frac{6}{5}\cdot\frac{8}{7}$, $\cdots$ sind, und zwar so, dass wir zu der Gleichung gelangen:

$$2=\frac{\pi}{\sqrt{2}}\cdot\frac{2}{3}\cdot\frac{6}{5}\cdot\frac{8}{7}\cdot\frac{10}{11}\cdot\frac{14}{13}\cdot\frac{16}{17}\cdot\frac{18}{19}\cdots,$$

wo die Nenner die natürliche Reihe der Primzahlen bilden, die Zähler aber um eine Einheit kleiner sind als die Nenner, sobald diese von der Form $8k+1$ oder $8k+3$, dagegen um eine Einheit grösser sind als die Nenner, sobald die letzteren von der Form $8k+5$ oder $8k+7$ sind.

II.

1.

Es sind schon sechsunddreissig Jahre verflossen, seit ich die Prinzipien des in dieser Abhandlung zu behandelnden wunderbaren Zusammenhanges entdeckt habe, wie ich schon am Schlusse der „*Arithmetischen Untersuchungen*“ bemerkte. Andere Beschäftigungen aber hatten mich lange Zeit hindurch von dieser Untersuchung abgezogen, bis ich erst kürzlich wieder zu ihr zurückzukehren und durch erneute Bemühungen sie zu erweitern vermochte. Da jedoch der Umfang dieses neuen Teils der höheren Arithmetik die Grenzen einer Abhandlung überschreitet, so soll diese erstere Abhandlung den Formen mit negativer Determinante gewidmet sein; die Formen mit positiver Determinante aber, welche eine ganz eigentümliche Behandlung erfordern, sollen einer zweiten Abhandlung vorbehalten bleiben.

2.

Zu unserm Zwecke bedürfen wir eines Satzes, der an sich zwar arithmetisch ist, dessen Natur man aber bequemer und deutlicher durch in geometrische Form gekleidete Betrachtungen vor Augen führen kann.

Ist in einer unendlichen Ebene eine durch eine irgend wie beschaffene Linie begrenzte Figur gegeben, so lässt sich ihr Flächeninhalt annähernd bestimmen, wenn man die Ebene in Quadrate teilt und die Anzahl sowohl derjenigen, welche ganz innerhalb der Figur liegen, als auch derjenigen, welche von dem Umfang der Figur geschnitten werden, zählt, und wird offenbar die Fläche mit Recht kleiner oder grösser sich ergeben, je nachdem die letzteren Quadrate entweder weggelassen oder zu den ersteren hinzugezählt werden. Wenn man aber die letzteren auf der Grenze gelegenen Quadrate nach Massgabe irgend welchen Prinzips teils ausschliessen teils zuzählen wollte, so wird der Fehler bald positiv bald negativ sein können, notwendig aber kleiner sein als das Aggregat aller auf der Grenze gelegenen Quadrate. Je kleiner die Quadrate genommen werden, um so genauer wird auf diese Weise die Fläche bestimmt werden, und eine derartige Annäherung wird man ins Unendliche fortsetzen oder die Quadrate so klein nehmen können, dass der Fehler kleiner wird als irgend eine gegebene Grösse. Obwohl dies schon an und für sich evident sein dürfte, wollen wir doch nicht verfehlen, es durch einen strengen Beweis zu begründen.

Je zwei Quadrate können entweder nur einen Winkelpunkt oder zwei oder gar keinen gemeinschaftlich haben; im ersten und zweiten Falle sollen sie einander benachbart, im dritten von einander getrennt heissen. Offenbar giebt es Quadrate, die sämtlich einander benachbart sind, nur je vier und daher müssen unter je fünf verschiedenen Quadraten wenigstens zwei von einander getrennte vorkommen. Da nun die Entfernung zwischen zwei in getrennten Quadraten liegenden Punkten nicht kleiner als die Seite der

Quadrate, die wir mit a bezeichnen wollen, sein kann, so wird offenbar, wenn ein Punkt, welcher von irgend einer Stelle eines Quadrats ausgegangen ist, der Reihe nach das zweite, dritte, vierte Quadrat durchschneidet und schliesslich zum fünften Quadrat gelangt, die Länge des Weges sicher nicht kleiner sein als a. Und da aus ähnlichem Grunde, wenn die Linie fortwährend andere Quadrate durchläuft, der Teil zwischen dem fünften und neunten Quadrat, ferner zwischen dem neunten und dreizehnten Quadrat u. s. w. nicht kleiner sein kann als a, so schliessen wir leicht, dass eine in sich zurückkehrende Linie, welche im Ganzen n verschiedene Quadrate berührt hat, sicher nicht kleiner als $\frac{(n-4)a}{4}$ sein kann. Umgekehrt also kann eine geschlossene Linie, deren Länge gleich l ist, sicher nicht mehr als $4+\frac{4l}{a}$ verschiedene Quadrate berührt haben. Da die Fläche dieser $=4a^2+4al$, wenn a ins Unendliche abnimmt, kleiner werden kann als jede gegebene Grösse, so gilt dasselbe umsomehr von dem Fehler der Quadratur, über die wir oben gesprochen haben.

3.

Ein Prinzip für die Zulassung oder Ausschliessung der auf der Grenze der Figur gelegenen Quadrate kann auf viele verschiedene Arten aufgestellt werden; das einfachste scheint jedoch zu sein, nur auf die Lage des Mittelpunktes eines jeden Quadrats Rücksicht zu nehmen, so dass die Quadrate, deren Mittelpunkte innerhalb der Figur liegen, zugelassen, diejenigen aber, deren Mittelpunkte ausserhalb der Figur sich befinden, ausgeschlossen werden, während es dem Belieben überlassen bleibt, ob man die Quadrate, deren Mittelpunkte zufällig auf der Peripherie selbst liegen, lieber zulassen oder ausschliessen will. An Stelle der Mittelpunkte könnte man auch jeden beliebigen andern in den einzelnen Quadraten analog gelegenen Punkt nehmen.

Auf diese Weise kommt die Sache darauf hinaus, dass wir uns in einer Ebene gleichweit von einander abstehende und auf äquidistanten Geraden derart gelegene Punkte denken, dass Quadrate entstehen. Ist dies geschehen, so können wir dem Satze des vorigen Artikels zufolge behaupten, dass die Anzahl der in der Figur enthaltenen Punkte multipliciert mit dem Quadrat der Entfernung zweier benachbarten Punkte, so nahe man will, gleich dem Flächeninhalt der Figur wird, wenn nur jene Entfernung hinreichend klein genommen wird, oder, um in der gewöhnlichen Redeweise zu sprechen, dass jenes Product die Fläche darstellt, wenn die Entfernung unendlich klein ist.

4.

Die Kurve, welche durch folgende Gleichung zwischen den rechtwinkligen Coordinaten p, q

$$ap^2+2bpq+cq^2=1$$

dargestellt wird, ist ein Kegelschnitt, und zwar eine Ellipse, wenn a, c und $ac - b^2$ positive Grössen sind; der von dieser Ellipse umschlossene Flächeninhalt findet sich $= \frac{\pi}{\sqrt{ac - b^2}}$. Der Wert der Grösse $ap^2 + 2bpq + cq^2$ ist ausserhalb der Ellipse überall grösser als 1, innerhalb der Ellipse kleiner als 1, negativ aber nirgends.

Man denke sich ein System von Punkten über die Ebene, in welcher die Ellipse gelegen ist, so zerstreut, dass sie Quadrate bilden, deren Seiten gleich λ und den Coordinatenachsen parallel sind, wobei es gleichgültig ist, ob der Coordinatenanfangspunkt oder der Mittelpunkt der Ellipse mit irgend einem dieser Punkte zusammenfällt oder nicht. Ist die Anzahl der Punkte innerhalb der Ellipse mit Hinzuzählung derjenigen, welche etwa auf der Peripherie gelegen sind, gleich m, so ist nach dem Satze des vorigen Artikels $\frac{\pi}{\sqrt{ac - b^2}}$ die Grenze der Grösse $m\lambda^2$, der sie sich, soweit man will, nähert, wenn λ ins Unendliche abnimmt.

Wenn man annimmt, dass der Anfangspunkt der Coordinaten mit irgend einem Punkte des Systems zusammenfällt, so werden, wenn man $p = \lambda x$, $q = \lambda y$ setzt, offenbar für die einzelnen Punkte des Systems x und y ganze Zahlen sein, und umgekehrt wird jede Combination ganzzahliger Werte der Grössen x, y irgend einem Punkte des Systems entsprechen. Hiernach ist die Zahl m nichts anderes, als die Anzahl aller Combinationen von ganzzahligen Werten der Grössen x, y, für welche F nicht grösser wird als M, wenn wir der Kürze wegen die Function oder die Form zweiten Grades $ax^2 + 2bxy + cy^2$ mit F und die Grösse $\frac{1}{\lambda^2}$ mit M bezeichnen. Die Determinante dieser Form ist $b^2 - ac$, wofür wir $-D$ schreiben werden. Daher wird unser Satz jetzt so auszusprechen sein.

Satz I. Die Anzahl m aller Combinationen von ganzzahligen Werten der Unbestimmten x, y, für welche der Wert einer Form mit der negativen Determinante $-D$ die Grenze M nicht überschreitet, wird gleich $\frac{\pi M}{\sqrt{D}}$, allerdings nur näherungsweise, aber mit einer ins Unendliche wachsenden Annäherung, wenn M ins Unendliche wächst. Es braucht kaum darauf hingewiesen zu werden, dass die unendliche Annäherung hier (und ebenso im Folgenden) nicht so zu verstehen ist, als ob die Differenz zwischen $\frac{\pi M}{\sqrt{D}}$ und m selbst ins Unendliche abnähme, vielmehr wird sich das Verhältnis zwischen diesen Grössen immer mehr der Einheit nähern, oder es wird $\frac{\pi M}{m\sqrt{D}} - 1$ ins Unendliche abnehmen.

5.

Um die Auszählung wirklich auszuführen, kann man so verfahren, dass für die einzelnen ganzen zwischen den Grenzen $-\sqrt{\frac{cM}{D}}$ und $+\sqrt{\frac{cM}{D}}$ gelegenen Werte von x je zwei der Gleichung $F=M$ entsprechende Werte von y berechnet werden, woraus man die Anzahl der ganzen zwischen diesen gelegenen Zahlen ohne Weiteres erhält. Da diese Anzahl für entgegengesetzte Werte von x dieselbe ist, so sind wir beinahe von der Hälfte der Arbeit befreit. Man kann die Sache auch so durchführen, dass man die Werte von x zählt, welche den einzelnen Werten von y zwischen den Grenzen $-\sqrt{\frac{aM}{D}}$ und $+\sqrt{\frac{aM}{D}}$ entsprechen. Durch zweckmässige Verbindung beider Methoden kann die Arbeit noch mehr erleichtert werden, was wir jedoch hier nicht ausführlicher darlegen; es möge genügen, wenn wir über den einfachsten Fall Einiges hinzufügen.

Ist die Form $F=x^2+y^2$ oder die Kurve ein Kreis und bezeichnen $r, r', r'', r''', \ldots, r^{(r)}$ die grössten ganzen Zahlen, welche respective kleiner sind als

$$\sqrt{M},\ \sqrt{M-1},\ \sqrt{M-4},\ \sqrt{M-9},\ \ldots,\ \sqrt{M-r^2},$$

oder diese selbst, wenn etwa unter diesen Grössen ganze Zahlen enthalten sind, so ist die gesuchte Anzahl:

$$\begin{aligned} m &= 2r+1+2(2r'+1)+2(2r''+1)+2(2r'''+1)+\cdots+2(r^{(r)}+1) \\ &= 1+4r+4r'+4r''+4r'''+\cdots+4r^{(r)}. \end{aligned}$$

Einfacher aber erreichen wir dasselbe, wenn wir mit q die grösste unterhalb $\sqrt{\frac{1}{2}M}$ (oder diese Grösse selbst, wenn sie eine ganze Zahl ist) liegende ganze Zahl bezeichnen, mit Hülfe der Formel:

$$m = 4q^2+1+4r+8(r^{(q+1)}+r^{(q+2)}+r^{(q+3)}+\cdots+r^{(r)}).$$

Auf diese Weise sind folgende Anzahlen ermittelt worden:

M	m	M	m	M	m
100	317	1 000	3 149	10 000	31 417
200	633	2 000	6 293	20 000	62 845
300	949	3 000	9 425	30 000	94 237
400	1 257	4 000	12 581	40 000	125 629
500	1 581	5 000	15 705	50 000	157 093
600	1 885	6 000	18 853	60 000	188 453
700	2 209	7 000	21 993	70 000	219 901
800	2 521	8 000	25 137	80 000	251 305
900	2 821	9 000	28 269	90 000	282 697
1 000	3 149	10 000	31 417	100 000	314 197.

6.

Den Satz des Artikels 4 verallgemeinern wir noch folgendermassen:

Satz II. Wenn nicht alle Combinationen von ganzzahligen Werten der Grössen x, y, für welche F den Wert M nicht überschreitet, zu sammeln sind, sondern nur in gewissen Zwischenräumen, nämlich diejenigen, in denen x einer gegebenen Zahl G nach einem gegebenen Modul g und y einer gegebenen Zahl H nach einem gegebenen Modul h congruent ist, so wird die Anzahl m' dieser Combinationen näherungsweise ausgedrückt werden durch $\frac{\pi M}{gh\sqrt{D}}$, und zwar wird die Annäherung ins Unendliche zunehmen, wenn M ins Unendliche wächst.

In der That setzt man $x = gx' + G$, $y = hy' + H$, so ist offenbar m' die Anzahl aller Combinationen ganzzahliger Werte der Grössen x', y', für welche

$$ag^2\left(x' + \frac{G}{g}\right)^2 + 2bgh\left(x' + \frac{G}{g}\right)\left(y' + \frac{H}{h}\right) + ch^2\left(y' + \frac{H}{h}\right)^2$$

den Wert M nicht überschreitet. Wenn wir daher in der Ebene uns ein System von Punkten denken, welches zwar ebenso wie im Artikel 4 verteilt ist, aber doch so, dass nicht der Anfangspunkt der Coordinaten sondern der Punkt, dessen Coordinaten $p = \frac{G\lambda}{g}$, $q = \frac{H\lambda}{h}$ sind, mit irgend einem Punkte des Systems zusammenfällt, so wird m' die Anzahl der Punkte innerhalb einer Ellipse, deren Gleichung

$$ag^2p^2 + 2bghpq + ch^2q^2 = 1$$

ist, mit Hinzurechnung der etwa auf der Peripherie selbst gelegenen Punkte ausdrücken. Und der Flächeninhalt dieser Ellipse, welcher gleich $\frac{\pi}{gh\sqrt{ac-b^2}} = \frac{\pi}{gh\sqrt{D}}$ ist, wird die Grenze sein, welcher sich das Product $m'\lambda^2 = \frac{m'}{M}$ ins Unendliche nähert, wenn λ ins Unendliche abnimmt oder M ins Unendliche wächst.

Übrigens ist klar, dass dieser Satz auch den Fall umfasst, wo nur die eine der beiden Unbestimmten x, y sprungweise fortschreiten soll, während der Wert der andern keiner Bedingung unterworfen ist. Denn offenbar ist dies dasselbe, als wenn entweder h oder g gleich 1 gesetzt wird.

7.

Die bisherigen Auseinandersetzungen sind von der Beschaffenheit der Coefficienten der Form $ax^2 + 2bxy + cy^2$ unabhängig; von jetzt an werden wir aber voraussetzen, dass diese Coefficienten ganze Zahlen seien. Auf

diese Weise wird jede Combination ganzzahliger Werte der Grössen x, y ganze Werte der Form selbst hervorbringen oder der Darstellung irgend einer ganzen Zahl durch jene Form entsprechen. Hieraus geht hervor, dass der Complex aller Combinationen von ganzzahligen Werten der Grössen x, y, durch welche die Form $F = ax^2 + 2bxy + cy^2$ einen die Grenze M nicht übersteigenden Wert erhält, derselbe ist wie der Complex aller Darstellungen der ganzen Zahlen, welche die Grenze M nicht überschreiten, oder der ganzen Zahlen bis zu dieser Grenze einschliesslich, wenn sie selbst eine ganze Zahl ist. Wenn wir daher der Kürze wegen die Anzahl der verschiedenen Darstellungen einer bestimmten ganzen Zahl n durch die Form F mit $F(n)$ oder, insofern eine Zweideutigkeit nicht zu befürchten ist, einfach mit Fn bezeichnen, so ist die oben durch m dargestellte Zahl gleich $F0 + F1 + F2 + F3 + \cdots + FM$, und der erste Satz nimmt die Form an:

Satz III. Das Aggregat $F0 + F1 + F2 + F3 + \cdots + FM$ wird näherungsweise ausgedrückt durch $\frac{\pi M}{\sqrt{D}}$, wo die Annäherung ins Unendliche zunimmt, wenn M ins Unendliche wächst.

8.

Zu dem dritten die Darstellungen aller Zahlen betreffenden Satze wollen wir noch einen andern hinzufügen, welcher sich nur auf die ungeraden Zahlen bezieht. Offenbar können durch die Form F keine ungeraden Zahlen dargestellt werden, wenn a und c gleichzeitig gerade Zahlen sind; daher ist die Untersuchung auf die übrigen drei Fälle beschränkt.

I. Sooft a ungerade, c gerade ist, wird eine ungerade Zahl dargestellt, wenn man x einen ungeraden Wert beilegt, während der Wert von y willkürlich bleibt. Daher lehrt der Satz II, wenn man $g = 2$, $G = 1$, $h = 1$ setzt, dass die Anzahl aller Combinationen solcher Werte von x, y, für welche die Form einen ungeraden die Grenze M nicht übersteigenden Wert erhält, bei ins Unendliche wachsendem M mit unendlicher Annäherung durch $\frac{\pi M}{2\sqrt{D}}$ dargestellt wird.

II. Ist a gerade, c ungerade, so ist zur Darstellung einer ungeraden Zahl erforderlich, dass y ungerade sei, weshalb wir, wenn wir $g = 1$, $h = 2$, $H = 1$ setzen, zu demselben Schlusse gelangen.

III. Ist sowohl a als auch c ungerade, so muss entweder ein ungerader Wert von x mit einem geraden Werte von y oder ein gerader Wert von x mit einem ungeraden Werte von y combiniert werden, damit sich ein ungerader Wert der Formel ergebe. Die Anzahl aller Combinationen sowohl der ersteren wie auch der letzteren Art, für welche der Wert der Form die Grenze M nicht überschreitet, wird mit unendlicher Annäherung durch

$\frac{\pi M}{4\sqrt{D}}$ ausgedrückt; mithin wird die Anzahl aller Combinationen, welche ungerade die Grenze M nicht überschreitende Werte der Form hervorbringen, auch hier mit unendlicher Annäherung durch $\frac{\pi M}{2\sqrt{D}}$ ausgedrückt.

Da nun der Complex aller solcher Combinationen nichts anderes ist, als der Complex aller Darstellungen aller Zahlen 1, 3, 5, 7, ..., M, sooft M eine ungerade ganze Zahl, oder aller Zahlen 1, 3, 5, 7, ..., $M-1$, sooft M eine gerade ganze Zahl ist, so haben wir den

Satz IV. Das Aggregat

$$F1+F3+F5+F7+\cdots+FM \text{ oder } F1+F3+F5+F7+\cdots+F(M-1),$$

je nachdem M ungerade oder gerade ist, wird mit unendlicher Annäherung ausgedrückt durch $\frac{\pi M}{2\sqrt{D}}$, falls F eine Form ist, in welcher der eine oder jeder der beiden Coefficienten a, c ungerade ist.

[III.]

Es sei C der Complex der Repräsentanten sämtlicher Klassen der eigentlich primitiven Formen für die Determinante $-D$. Wir bezeichnen durch (n) die Anzahl aller Darstellungen der Zahl n durch Formen aus dem Complex C. Es sei p eine ungerade Primzahl. Dann ist

1. $(pn) = (n)$, wenn p ein Teiler von D,
2. $(pn) = (n) + (h)$ } wenn p Nichtteiler von D { Teiler von x^2+D,
3. $(pn) = -(n) + (h)$ } wenn p Nichtteiler von D { Nichtteiler von x^2+D,

wo $n = hp^\mu$, μ beliebig und h nicht teilbar durch p.

Im Falle 1. ist: $(h) = (ph) = (p^2h) = (p^3h) = \cdots$
" " 2. " $(ph) = 2(h)$, $(p^2h) = 3(h)$, $(p^3h) = 4(h)$, $\cdots$
" " 3. " $(ph) = 0$, $(p^2h) = (h)$, $(p^3h) = 0$, $(p^4h) = (h)$, $\cdots$

* * *

Aus jeder eigentlich primitiven Klasse für die Determinante $-D$, deren Anzahl $= \lambda$, sei eine Form ausgewählt, und der Complex dieser Formen sei L.

Man bezeichne durch $f(A)$ die Anzahl sämtlicher Darstellungen der Zahl A durch Formen aus L.

Es sei ferner $f(A;\, p) = f\left(\frac{A}{p^\alpha}\right)$, wenn p^α die höchste Potenz der Primzahl p ist, welche in A aufgeht; ferner $f(A;\, p, q) = f\left(\frac{A}{p^\alpha q^\beta}\right)$, wenn q

eine andere Primzahl ist, deren höchste in A aufgehende Potenz $= q^\beta$, und so ferner $f(A;\, p, q, r) = f\left(\frac{A}{p^\alpha q^\beta r^\gamma}\right)$, wenn r eine dritte Primzahl, deren höchste in A aufgehende Potenz r^γ ist, u. s. w.

[IV.]

Man bezeichne durch (n) die Anzahl der Werte x aus dem Complexe

$$0,\ 1,\ 2,\ 3,\ 4,\ \ldots,\ p^n - 1,$$

für welche $x^2 - D = x^2 - ap^\mu$ durch p^n teilbar ist.

1) μ ungerade z. B. $= 7$.	2) μ gerade z. B. $= 6$	
	aNp	aRp
$(1) = 1$	$(1) = 1$	$(1) = 1$
$(2) = p$	$(2) = p$	$(2) = p$
$(3) = p$	$(3) = p$	$(3) = p$
$(4) = p^2$	$(4) = p^2$	$(4) = p^2$
$(5) = p^2$	$(5) = p^2$	$(5) = p^2$
$(6) = p^3$	$(6) = p^3$	$(6) = p^3$
$(7) = p^3$	$(7) = 0$	$(7) = 2p^3$
$(8) = 0$	$(8) = 0$	$(8) = 2p^3$
$(9) = 0$		
u. s. w.	u. s. w.	u. s. w.

Man mache nun:

$$(1) - \frac{(2)}{p} = (1)'$$
$$(2) - \frac{(3)}{p} = (2)'$$
$$(3) - \frac{(4)}{p} = (3)'$$
$$(4) - \frac{(5)}{p} = (4)'$$

u. s. w.

dann ist:

$$f(p) = (1)'$$
$$f(p^2) = 1 + (2)'$$
$$f(p^3) = (1)' + (3)'$$
$$f(p^4) = 1 + (2)' + (4)'$$

u. s. w.

Es ist folglich,

$$\frac{p-1}{p}\left(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \frac{f(p^3)}{p^3} + \cdots\right) = T \text{ gesetzt,}$$

$$\frac{p+1}{p}\,T = 1 + \frac{(1)'}{p} + \frac{(2)'}{p^2} + \frac{(3)'}{p^3} + \frac{(4)'}{p^4} + \cdots = 1 + \frac{(1)}{p} = 1 + \frac{1}{p}.$$

Also $T = 1$.

[V.]

Die mittlere Anzahl der Klassen*) für die negative Determinante $-D$ ist sehr nahe

$$=\frac{\pi\sqrt{D}}{4(1+\frac{1}{27}+\frac{1}{125}+\cdots)}.$$

Die wahre Anzahl aber wird durch folgende Formeln ausgedrückt, wo der Kürze wegen m für die mittlere, M für die wahre Anzahl geschrieben ist; p, q stellen sämtliche ungeraden in D nicht aufgehenden Primzahlen dar, und zwar jenes die Teiler, dieses die Nichtteiler von x^2+D; r bedeutet die in D aufgehenden Primzahlen.**)

I. $M = m \times$ Product aus $\frac{p^3+p^2}{p^3-1}\cdot\frac{q^3-q^2}{q^3-1}\cdot\frac{r^3-r}{r^3-1}$

II. $M = \frac{\pi\sqrt{D}}{4} \times$ Product aus $\frac{p+1}{p}\cdot\frac{q-1}{q}\cdot\frac{r^2-1}{r^2}$

III. NB. $M = \frac{2\sqrt{D}}{\pi} \times$ Product aus $\frac{p}{p-1}\cdot\frac{q}{q+1}$

IV. $M = \sqrt{\frac{D}{2}} \times$ Product aus $\frac{p+1}{p-1}\cdot\frac{q-1}{q+1}\cdot\frac{r^2-1}{r^2}$

V. $M = \frac{2\sqrt{D}}{\pi}\left\{1\pm\frac{1}{3}\pm\frac{1}{5}\pm\frac{1}{7}\pm\frac{1}{9}\pm\cdots\right\}.$

NB. Die Formel III wird unmittelbar aus der Vergleichung der beiden Arten, die darstellbaren Zahlen bis zu einer gewissen Grenze zu zählen, abgeleitet.

[VI.]

Satz. Die Anzahl der Klassen, in welche sämtliche eigentlich primitiven binären Formen für die negative Determinante $-D$ zerfallen, ist gleich

$$\frac{\pi}{4}\times\sqrt{D}\times \text{Product aus } \frac{p-1}{p}\cdot\frac{q+1}{q}\times\frac{r^2-1}{r^2},$$

*) [Vgl. *„Arithmet. Unters.“*, Art. 302 (oben S. 350); die dortige Formel weicht um eine Constante δ von der hier im Text vorkommenden ab.]

**) [ungeraden.]

wo bezeichnet:

p alle [ungeraden] Primzahlen, deren Nichtrest $-D$ ist,
q alle [ungeraden] Primzahlen, deren Rest $-D$ ist,
r alle [ungeraden] in D aufgehenden Primzahlen;

$$= \frac{\frac{\pi}{4}\sqrt{D} \times \text{Product aus } \frac{r^2-1}{r^2}}{1 \pm \frac{1}{3} \pm \frac{1}{5} \pm \cdots},$$

wo im Nenner das positive Vorzeichen denjenigen Brüchen, deren Nenner unter der Form der Nichtteiler, das negative aber denjenigen vorzusetzen ist, deren Nenner unter der Form der Teiler von x^2+D enthalten sind; diejenigen Brüche aber, deren Nenner zu D nicht prim sein würden, sind ganz wegzulassen.*)

$$= \frac{2\sqrt{D}(1 \pm \frac{1}{3} \pm \frac{1}{5} \pm \cdots)}{\pi} = \frac{\operatorname{cotg}\vartheta \pm \operatorname{cotg}3\vartheta \pm \operatorname{cotg}5\vartheta \pm \cdots \pm \operatorname{cotg} n\vartheta}{N:\sqrt{D}},$$

wenn man setzt $\vartheta = \frac{\pi}{N}$, $N = \left\{\begin{matrix}1\\4\end{matrix}\right\} D$ und für n alle zu D primen Zahlen mit dem wie oben bestimmten Vorzeichen nimmt.**)

Für positive Determinanten ist die Anzahl der Klassen***)

$$= \frac{2\sqrt{D}(1 \pm \frac{1}{3} \pm \frac{1}{5} \pm \cdots)}{\log(T+U\sqrt{D})},$$

---

*) [Bezeichnet man mit m alle positiven ganzen Zahlen, die relative Primzahlen zu $2D$ sind, und benutzt man das durch Jacobi verallgemeinerte Symbol von Legendre, so ist die obige Regel für die Zeichenbestimmung in folgender Weise zu berichtigen: in der vorhergehenden Formel ist der Nenner:

$$1 \pm \frac{1}{3} \pm \frac{1}{5} \pm \cdots = \Sigma \pm \left(\frac{-D}{m}\right)\frac{1}{m},$$

wo das obere oder untere Zeichen zu nehmen ist, je nachdem die Zahl m ein Product aus einer geraden oder ungeraden Anzahl (gleicher oder ungleicher) Primzahlen ist; dagegen ist im Zähler der nachfolgenden Formel:

$$1 \pm \frac{1}{3} \pm \frac{1}{5} \pm \cdots = \Sigma \left(\frac{-D}{m}\right)\frac{1}{m}\,]$$

**) [Siehe die weiter unten folgende Note zu diesem Fragment.]

***) [In der nachfolgenden Formel bedeutet D die positive Determinante und es ist:

$$1 \pm \frac{1}{3} \pm \frac{1}{5} \pm \cdots = \Sigma \left(\frac{D}{m}\right)\frac{1}{m}\,]$$

wo T, U die kleinsten der Gleichung $t^2 - Du^2 = 1$ genügenden Werte der Grössen t, u bezeichnen.

$$= \frac{\log\sin\frac{1}{2}\vartheta \pm \log\sin\frac{3}{2}\vartheta \pm \log\sin\frac{5}{2}\vartheta \pm \cdots}{\log(T+U\sqrt{D})}.$$

[VII.]

Für eine negative Determinante $-p$, welche*) eine Primzahl von der Form $4n+1$ ist, ist die Anzahl der Klassen**) $= (\alpha - \beta)$, wo α die Anzahl der quadratischen Reste im ersten Quadranten

$$1,\ 2\cdot 3 \cdots \tfrac{1}{4}(p-1),$$

β die Anzahl der Nichtreste bezeichnet.

[VIII.]

$$b \equiv 2m + a - 1 \pmod{8},$$

wo m die [halbe] Anzahl der Klassen für die Determinante $-p$ ist.

p	m	a	b	f	$\frac{2m+a-1-b}{8}$	α	β
17	2	+ 1	− 4	− 4	+ 1	3	2
41	4	+ 5	+ 4	+ 9	+ 1	3	4
73	2	− 3	− 8	+ 27	+ 1	1	6
89	6	+ 5	− 8	+ 34	+ 3	9	2
97	2	+ 9	+ 4	+ 22	+ 1	5	6
113	4	− 7	+ 8	+ 15	− 1	9	4
137	4	− 11	+ 4	+ 37	− 1	3	8
193	2	− 7	+ 12	+ 81	− 2	11	6
233	6	+ 13	+ 8	+ 144	+ 2	15	2
241	6	+ 15	+ 4	+ 64	− 1	13	6
257	8	+ 1	+ 16	+ 16	0	15	4
281	10	+ 5	− 16	+ 53	+ 5	9	10
313	4	+ 13	− 12	− 25	+ 1	5	12
337	4	+ 9	+ 16	− 148	0	7	12
353	8	+ 17	+ 8	+ 42	+ 3	15	8
5	1	+ 1	+ 2	+ 2	0		
13	1	− 3	− 2	+ 5	0		
29	3	+ 5	+ 2	+ 12	+ 1		

*) [d. h. wenn p eine positive Primzahl von der Form $4n+1$ ist.]

**) [Die Anzahl der Klassen ist $= 2(\alpha - \beta)$].

p	m	a	b	f	$\frac{2m+a-1-b}{8}$	α	β
37	1	+ 1	− 6	− 6	+ 1		
53	3	− 7	− 2	+ 23	0		
61	3	+ 5	− 6	+ 11	+ 2		
101	7	+ 1	− 10	− 10	+ 3		
109	3	− 3	+ 10	+ 33	− 1		
149	7	− 7	− 10	+ 44	+ 2		
157	3	− 11	− 6	− 28	0		
173	7	+ 13	+ 2	+ 80	+ 3		
181	5	+ 9	+ 10	− 19	+ 1		
197	5	+ 1	− 14	− 14	+ 3		
229	5	− 15	+ 2	− 107	− 1		
269	11	+ 13	+ 10	− 82	+ 3		
277	3	+ 9	+ 14	− 60	0		
293	9	+ 17	+ 2	+ 138	+ 4		
317	5	− 11	+ 14	+ 114	− 2		
349	7	+ 5	+ 18	− 136	0		
373	5	− 7	+ 18	+ 104	− 2		
389	11	+ 17	− 10	− 115	+ 6		
397	3	− 19	− 6	+ 63	− 1		

[IX.]

Verteilung der quadratischen Reste in Octanten.

p Primzahl; (r) Anzahl der quadratischen Reste von p, welche zwischen $(r-1)\frac{p}{8}$ und $r\frac{p}{8}$ liegen.

Erster Fall; $p = 8n+1$.

$2t$ Anzahl der Klassen für die Determinante $-p$
$2u$ Anzahl der Klassen für die Determinante $-2p$

$$(1) = (8) = \tfrac{1}{4}(2n+t+u)$$
$$(2) = (4) = (5) = (7) = \tfrac{1}{4}(2n+t-u)$$
$$(3) = (6) = \tfrac{1}{4}(2n-3t+u).$$

p	$2n$	t	u	(1)	(2)	(3)	p	$2n$	t	u	(1)	(2)	(3)
17	4	2	2	2	1	0	233	58	6	4	17	15	11
41	10	4	2	4	3	0	241	60	6	10	19	14	13
73	18	2	8	7	3	5	257	64	8	8	20	16	12
89	22	6	4	8	6	2	281	70	10	4	21	19	11
97	24	2	10	9	4	7	313	78	4	18	25	16	21
113	28	4	4	9	7	5	337	84	4	12	25	19	21
137	34	4	6	11	8	7	353	88	8	12	27	21	19
193	48	2	10	15	10	13	401	100	10	6	29	26	19

Zweiter Fall. $p = 8n + 5$.

$2t$ Anzahl der Klassen für die Determinante $-p$;
$2u$ Anzahl der Klassen für die Determinante $-2p$.

$$(1) = (3) = (6) = (8) = \tfrac{1}{4}(2n - t + u)$$
$$(2) = (7) = \tfrac{1}{4}(2n + 3t - u + 2)$$
$$(4) = (5) = \tfrac{1}{4}(2n - t - u + 2).$$

p	$2n$	t	u	(1)	(2)	(4)	p	$2n$	t	u	(1)	(2)	(4)
5	0	1	1	0	1	0	181	44	5	9	12	13	8
13	2	1	3	1	1	0	197	58	5	5	12	15	10
29	6	3	1	1	4	1	229	56	5	13	16	15	10
37	8	1	5	3	2	1	269	66	11	5	15	24	13
53	12	3	3	3	5	2	277	68	3	11	19	17	14
61	14	3	5	4	5	2	293	72	9	9	18	23	14
101	24	7	3	5	11	4	317	78	5	7	20	22	17
109	26	3	5	7	8	5	349	86	7	13	23	24	17
149	36	7	3	8	14	7	373	92	5	13	25	24	19
157	38	3	13	12	9	6	389	96	11	7	23	31	20
173	42	7	5	10	15	8	397	98	3	21	29	22	19

Dritter Fall. $p = 8n + 3$.

t Anzahl der Klassen für die Determinante $-p$
$2u$ Anzahl der Klassen für die Determinante $-2p$.

$$(1) = (4) = (7) = \tfrac{1}{4}(2n + t - u)$$
$$(2) = (5) = (8) = \tfrac{1}{4}(2n - t + u)$$
$$(3) \quad = \tfrac{1}{4}(2n + t + u + 2)$$
$$(6) \quad = \tfrac{1}{4}(2n - t - u + 2).$$

p	$2n$	t	u	(1)	(2)	(3)	(6)	p	$2n$	t	u	(1)	(2)	(3)	(6)
3	0	1	1	0	0	1	0	163	40	3	11	8	12	14	7
11	2	3	1	1	0	2	0	179	44	15	3	14	8	16	7
19	4	3	3	1	1	3	0	211	52	9	5	14	12	17	10
43	10	3	5	2	3	5	1	227	56	15	7	16	12	20	9
59	14	9	3	5	2	7	1	251	62	21	7	19	12	23	9
67	16	3	7	3	5	7	2	283	70	9	15	16	19	24	12
83	20	9	5	6	4	9	2	307	76	9	17	17	21	26	13
107	26	9	3	8	5	10	4	331	82	9	11	20	21	26	16
131	32	15	3	11	5	13	4	347	86	15	5	24	19	27	17
139	34	9	7	9	8	13	5	379	94	9	11	23	24	29	19

Vierter Fall. $p = 8n + 7$.

t Anzahl der Klassen für die Determinante $-p$
$2u$ Anzahl der Klassen für die Determinante $-2p$.

$$(1) = \tfrac{1}{4}(2n + 2t - u)$$
$$(2) = (3) = (5) = \tfrac{1}{4}(2n + u + 2)$$
$$(4) = (6) = (7) = \tfrac{1}{4}(2n - u + 2)$$
$$(8) = \tfrac{1}{4}(2n - 2t + u).$$

p	$2n$	t	u	(1)	(2)	(4)	(8)	p	$2n$	t	u	(1)	(2)	(4)	(8)
7	0	1	2	0	1	0	0	191	46	13	4	17	13	11	6
23	4	3	2	2	2	1	0	199	48	9	10	14	15	10	10
31	6	3	4	2	3	1	1	223	54	7	16	13	18	10	14
47	10	5	4	4	4	2	1	239	58	15	4	21	16	14	8
71	16	7	2	7	5	4	1	263	64	13	6	21	18	15	11
79	18	5	4	6	6	4	3	271	66	11	12	19	20	14	14
103	24	5	10	6	9	4	6	311	76	19	6	27	21	18	11
127	30	5	8	8	10	6	7	359	88	19	6	30	24	21	14
151	36	7	6	11	11	8	7	367	90	9	20	22	28	18	23
167	40	11	6	14	12	9	6	383	94	17	12	29	27	21	18

[X.]

Verteilung der quadratischen Reste in Zwölftel.

p Primzahl; (r) Anzahl der quadratischen Reste von p, welche zwischen $\frac{r-1}{12}p$ und $\frac{r}{12}p$ liegen.

Erster Fall. $p = 24n + 1$.

$2t$ Anzahl der Klassen für die Determinante $-p$
$4u$ Anzahl der Klassen für die Determinante $-3p$.

$$(1) = (12) = \tfrac{1}{6}(6n + 3t + 2u)$$
$$(2) = (4) = (6) = (7) = (9) = (11) = \tfrac{1}{6}(6n - 3t + 2u)$$
$$(3) = (5) = (8) = (10) = \tfrac{1}{6}(6n + 3t - 4u)$$

p	n	t	u	(1)	(2)	(3)
73	3	2	3	5	3	2
97	4	2	3	6	4	3
193	8	2	6	11	9	5
241	10	6	3	14	8	11

Zweiter Fall. $p = 24n + 13$.

$2t$ Anzahl der Klassen für die Determinante $-p$
$4u$ Anzahl der Klassen für die Determinante $-3p$.

$$(1) = (3) = (10) = (12) = \tfrac{1}{2}(2n + 1 + t)$$
$$(2) = (6) = (7) = (11) = \tfrac{1}{2}(2n + 1 - t)$$
$$(4) = (9) = \tfrac{1}{2}(2n + 1 - t + 2u)$$
$$(5) = (8) = \tfrac{1}{2}(2n + 1 + t - 2u).$$

p	n	t	u	(1)	(2)	(4)	(5)
13	0	1	1	1	0	1	0
37	1	1	2	2	1	3	0
61	2	3	2	4	1	3	2
109	4	3	3	6	3	6	3
157	6	3	4	8	5	9	4
181	7	5	3	10	5	8	7
229	9	5	3	12	7	10	9

Dritter Fall. $p = 24n + 5$.

$2t$ Anzahl der Klassen für die Determinante $-p$
$2u$ Anzahl der Klassen für die Determinante $-3p$

$$(1) = (2) = (6) = (7) = (11) = (12) = n$$
$$(3) = (10) = \tfrac{1}{2}(2n + 1 + t)$$
$$(4) = (9) = \tfrac{1}{2}(2n - t + u)$$
$$(5) = (8) = \tfrac{1}{2}(2n + 1 - u).$$

p	n	t	u	(1)	(3)	(4)	(5)
5	0	1	1	0	1	0	0
29	1	3	3	1	3	1	0
53	2	3	5	2	4	3	0
101	4	7	5	4	8	3	2
149	6	7	7	6	10	6	3
173	7	7	9	7	11	8	3
197	8	5	11	8	11	11	3
269	11	11	7	11	17	9	8

Vierter Fall. $p = 24n + 17$.

$2t$ Anzahl der Klassen für die Determinante $-p$
$2u$ Anzahl der Klassen für die Determinante $-3p$.

$$(1) = (2) = (6) = (7) = (11) = (12) = \tfrac{1}{6}(6n + 3 + u)$$
$$(3) = (10) \qquad = \tfrac{1}{6}(6n + 6 + 3t - 2u)$$
$$(4) = (9) \qquad = \tfrac{1}{6}(6n + 3 - 3t + u)$$
$$(5) = (8) \qquad = \tfrac{1}{6}(6n + 6 - 2u).$$

p	n	t	u	(1)	(3)	(4)	(5)
17	0	2	3	1	1	0	0
41	1	4	3	2	3	0	1
89	3	6	3	4	6	1	3
113	4	4	9	6	4	4	2
137	5	4	9	7	5	5	3
233	9	6	15	12	8	9	5
257	10	8	9	12	12	8	8

Eingehendere Betrachtung gewisser auf die Teilung des Kreises bezüglicher Untersuchungen.

367.*)

Was wir im letzten Teile des siebenten Abschnitts von Artikel 355 an dargelegt haben, stellt jedenfalls schwerwiegende Proben von der grossen Fruchtbarkeit der Lehre von der Teilung des Kreises sowie von dem wunderbaren Zusammenhange dar, welcher diese Disziplin mit verschiedenen arithmetischen Untersuchungen verbindet. Wir konnten daselbst aber, an Raum und Zeit allzusehr beschränkt, dieses Feld, welches unsere Bemühungen durch um so reichere Ernte belohnt, je weiter wir in ihm fortschreiten, nur leise streifen. Wir beabsichtigen daher, eine oder die andere der dort begonnenen Untersuchungen hier von Neuem wieder aufzunehmen und ausführlicher zu behandeln, und sicherlich wird der Leser nicht ohne grosses Staunen sehen, dass die Lösung mehrerer Probleme, die Jedermann für himmelweit hiervon verschieden gehalten hätte, auf diesem Fundamente ruht.

368.

Den fruchtbarsten Gegenstand liefert die im Artikel 356 angefangene Untersuchung, wo wir, nachdem der Complex der Wurzeln der Gleichung $x^n - 1 = 0$ (mit Ausschluss der Einheit) in zwei Klassen geteilt worden war, das Aggregat in jeder der beiden Klassen zu bestimmen lehrten, und zwar ergaben sich dieselben $= -\frac{1}{2} + \frac{1}{2}\sqrt{n}$ und $-\frac{1}{2} - \frac{1}{2}\sqrt{n}$ für den Fall, wo n von der Form $4n+1$, oder $= -\frac{1}{2} + \frac{1}{2}\sqrt{-n}$ und $-\frac{1}{2} - \frac{1}{2}\sqrt{-n}$ für den Fall, wo n von der Form $4n+3$ ist. Indessen hatten wir uns daselbst nicht allein die Beschränkung auf den Fall, wo n eine Primzahl ist, auferlegt, sondern auch, was von noch viel schwererer Bedeutung ist, das

*) Vgl. das Vorwort des Herausgebers.

Vorzeichen der Wurzelgrösse unbestimmt gelassen oder hatten es vielmehr verabsäumt, diese nur kurz angedeutete Bestimmung durch einen strengen Beweis zu bekräftigen. Diese Lücke müssen wir daher vor Allem ausfüllen.

369.

Es sei nun also n eine beliebige ganze positive Zahl, R eine solche Wurzel der Gleichung $x^n - 1 = 0$, dass keine niedrigere Potenz von ihr als die n^{te} der Einheit gleich wird (vgl. Artikel 359, II, oben S. 434), und es werde mit $[\lambda]$, wie im siebenten Abschnitt, die Potenz R^λ bezeichnet, so dass $[0] = 1$, $[1], [2], [3], \ldots, [n-1]$ sämtliche Wurzeln der Gleichung $x^n - 1 = 0$ darstellen. Ferner bezeichnen wir das Aggregat

$$[0] + [1] + [4] + [9] + \cdots + [(n-1)^2] \text{ mit } \Sigma[\mathfrak{Q}]$$

und allgemeiner

$$[0] + [\lambda] + [4\lambda] + [9\lambda] + \cdots + [\lambda(n-1)^2] \text{ mit } \Sigma[\mathfrak{Q}\lambda],$$

so dass $\mathfrak{Q}$ unbestimmt die Quadrate der Zahlen $0, 1, 2, 3, \ldots, n-1$ bedeutet. Offenbar wird also, ebenso wie allgemein $[\lambda] = [\mu]$ ist, wenn λ, μ irgend welche (positive oder negative) nach dem Modul n congruente ganze Zahlen sind, auch $\Sigma[\mathfrak{Q}\lambda] = \Sigma[\mathfrak{Q}\mu]$ sein, wenn $\lambda \equiv \mu$ ist. Nach diesen Vorbereitungen haben wir die folgende Aufgabe.

370.

Aufgabe. Das Product aus den beiden Aggregaten $\Sigma[\mathfrak{Q}]$ und $\Sigma[-\mathfrak{Q}]$ zu bestimmen.

Auflösung. Da $n^2 \equiv 0$, $(n+1)^2 \equiv 1$, $(n+2)^2 \equiv 4, \ldots$ (mod. n) ist, so ergiebt sich leicht, dass

$$\begin{aligned}\Sigma[\mathfrak{Q}] &= [1] + [4] + [9] + [16] + \cdots + [n^2] \\ &= [4] + [9] + [16] + [25] + \cdots + [(n+1)^2] \\ &= [9] + [16] + [25] + [36] + \cdots + [(n+2)^2] \\ &\quad \ldots\ldots\ldots\ldots\ldots\ldots \text{ oder allgemein} \\ &= [k^2] + [(k+1)^2] + [(k+2)^2] + [(k+3)^2] + \cdots + [(n+k-1)^2]\end{aligned}$$

wird. Hieraus ist:

$$[-k^2] \times \Sigma[\mathfrak{Q}] = [0] + [2k+1] + [4k+4] + [6k+9] + \cdots + [(n-1)^2 + 2(n-1)k].$$

Demnach entwickelt sich $\Sigma[-\mathfrak{Q}] \times \Sigma[\mathfrak{Q}]$ in

$$\begin{aligned}&+ [0] + [1] + [4] + [9] + \cdots + [(n-1)^2] \\ &+ [0] + [3] + [8] + [15] + \cdots + [n^2 - 1] \\ &+ [0] + [5] + [12] + [21] + \cdots + [n^2 + 2n - 3] \\ &+ [0] + [7] + [16] + [27] + \cdots + [n^2 + 4n - 5] \\ &+ \ldots\ldots\ldots\ldots\ldots\ldots \\ &+ [0] + [2n-1] + [4n] + [6n+3] + \cdots + [3n^2 - 6n + 3]\end{aligned}$$

Summiert man die einzelnen Vertikalreihen, so erhält man:

$$n[0]+[1]\frac{1-[2n]}{1-[2]}+[4]\frac{1-[4n]}{1-[4]}+[9]\frac{1-[6n]}{1-[6]}+\cdots+[(n-1)^2]\frac{1-[2n^2-2n]}{1-[2n-2]},$$

und in diesem Ausdrucke werden alle Teile ausser dem ersten verschwinden, wenn n ungerade ist, denn dann werden alle Zähler $1-[2n]$, $1-[4n]$, $1-[6n], \ldots$, dagegen keiner der Nenner $1-[2]$, $1-[4]$, $1-[6]$, $1-[8], \ldots, 1-[2n-2]$ gleich Null. Ist aber n eine gerade Zahl, so ist auch unter den Nennern einer gleich 0, nämlich $1-[n]$, welchem das Glied $[\frac{1}{4}n^2]\cdot\frac{1-[n^2]}{1-[n]}$ entspricht; die Summe der Teile aber, aus denen dieses entstanden ist, wird gleich $n[\frac{1}{4}n^2]$. Hier sind von Neuem zwei Fälle zu unterscheiden. Ist n gerademal gerade, so wird $\frac{1}{4}n^2\equiv 0 \pmod{n}$ und daher $[\frac{1}{4}n^2]=1$; ist aber n ungerademal gerade, so wird $\frac{1}{4}n^2\equiv\frac{1}{2}n \pmod{n}$ und daher notwendig $[\frac{1}{4}n^2]=-1$. Hieraus folgt endlich:

1. Für einen ungeraden Wert von n wird das gesuchte Product $=n$;
2. Für einen gerademal geraden Wert von n wird dasselbe $=2n$;
3. Für einen ungerademal geraden Wert von n wird dasselbe $=0$.

371.

Es verlohnt sich, die Natur des Aggregates $\Sigma[\mathfrak{Q}]$ näher zu betrachten.

I. Da man für die Quadrate 0, 1, 4, 9, 16, . . . ihre kleinsten Reste nach dem Modul n substituieren kann, so ist ersichtlich, dass, wenn M unbestimmt die quadratischen Reste von n unter den Zahlen 0 bis $n-1$ und m die Anzahl der Wurzeln der Congruenz $x^2\equiv M \pmod{n}$ bezeichnet, $\Sigma[\mathfrak{Q}]=\Sigma m[M]$ wird. Wie die Zahl m bestimmt wird, haben wir in den Artikeln 104 und 105 gezeigt (vgl. oben S. 72 u. 73).

II. Ist n eine (ungerade) Primzahl, so wird für $M\equiv 0: m=1$, für jeden andern Wert von M aber $m=2$. Ist aber n eine Potenz einer ungeraden Primzahl, etwa gleich p^ν, so wird $m=2$ für jeden durch p nicht teilbaren Wert von M, — — — — — — — — — — — —

372.

Ist n eine (ungerade) Primzahl, so bestehen die Reste M aus der Null, für welche $m=1$ ist, und $\frac{1}{2}(n-1)$ andern Zahlen, für welche $m=2$ ist. Bezeichnet man diese Reste (mit Ausschluss des Restes 0) unbestimmt durch μ, so ist unsere Reihe $=1+2\Sigma r^\mu$. Bezeichnet man ferner mit ν unbestimmt alle übrigen Zahlen unterhalb n, deren Anzahl ebenfalls gleich $\frac{1}{2}(n-1)$ ist und welche sämtliche quadratischen Nichtreste von n unterhalb n umfassen, so ist offenbar:

$$1+\Sigma r^\mu+\Sigma r^\nu = 1+r+r^2+r^3+\cdots+r^{n-1}=\frac{1-r^n}{1-r}=0.$$

Setzt man daher die Summe unserer Reihe oder $1 + 2\Sigma r^{\mu} = A$, so wird: $1 + 2\Sigma r^{\nu} = -A$ sowie $\Sigma r^{\mu} - \Sigma r^{\nu} = A$.

Nach Artikel 356 wird somit $A = \pm\sqrt{n}$ oder $= \pm\sqrt{-n}$, je nachdem $n \equiv 1$ oder $\equiv 3$ (mod. 4) ist. Das Vorzeichen aber wird hierdurch noch nicht bestimmt.

Substituiert man in unserer Reihe, die wir durch II bezeichnen wollen, für r eine andere gleichartige Wurzel der Gleichung $x^n - 1 = 0$, etwa $r' = r^{\lambda}$, so möge daraus die Reihe II′ hervorgehen.

373.

Wenn n das Quadrat oder eine höhere Potenz einer Primzahl, etwa $= p^{\pi}$ ist, so werden einige der Reste M aus den durch p nicht teilbaren Zahlen bestehen, andere werden durch p^2 aber nicht durch eine höhere Potenz von p teilbar sein, wieder andere werden sich durch p^4 aber nicht durch p^5 teilen lassen und so fort bis zu denen, welche durch $p^{\pi-2}$ aber nicht durch $p^{\pi-1}$ oder durch $p^{\pi-1}$ aber nicht durch p^{π}, je nachdem π gerade oder ungerade ist, teilbar sind; hierzu tritt endlich noch der Rest 0, welcher der einzige durch p^{π} teilbare ist (vgl. Artikel 102, oben S. 70). Bezeichnet man nun mit μ unbestimmt die quadratischen Reste der Zahl p unterhalb p mit Ausschluss der Null (deren Anzahl $= \frac{1}{2}(p-1)$ ist), so werden jene verschiedenen Arten von Resten folgendermassen dargestellt werden. Die ersten, welche durch p nicht teilbar sind, werden dargestellt durch $\mu + kp$, wo für k alle ganzen Zahlen von 0 bis $p^{\pi-1} - 1$ zu setzen sind, so dass die Anzahl aller in dieser Form enthaltenen Reste $= \frac{1}{2}(p-1)p^{\pi-1}$ ist; für jeden dieser wird $m = 2$. Die Summe aller in II diesen Resten entsprechenden Glieder ist gleich

$$2\Sigma r^{\mu+kp} = 2\Sigma r^{\mu} \cdot \Sigma r^{kp} = 2\Sigma r^{\mu} \cdot \frac{r^{p^{\pi}} - 1}{r^{p} - 1} = 0.$$

Die zweite Klasse der Reste wird dargestellt durch $\mu p^2 + kp^3$, wo für k alle ganzen Zahlen von 0 bis $p^{\pi-3} - 1$ zu setzen sind, so dass die Anzahl aller in dieser Form enthaltenen Reste $= \frac{1}{2}(p-1)p^{\pi-3}$ ist; für jeden einzelnen aber wird $m = 2p$. Die Summe der hieraus entstehenden Glieder in II wird gleich

$$2p\Sigma r^{\mu p^2 + kp^3} = 2p\Sigma r^{\mu p^2} \cdot \Sigma r^{kp^3} = 2p\Sigma r^{\mu p^2} \cdot \frac{r^{p^{\pi}} - 1}{r^{p^3} - 1} = 0,$$

wofern $\pi > 3$ ist. In analoger Weise wird die dritte, vierte u. s. w. Klasse dargestellt durch $\mu p^4 + kp^5$, $\mu p^6 + kp^7$, ..., wo für k alle ganzen Zahlen von 0 bis zu $p^{\pi-5} - 1$, $p^{\pi-7} - 1$, ... respective genommen werden müssen;

für diese wird $m = 2p^2$, $m = 2p^3$, ... Und die Summe der aus der dritten, vierten, u. s. w. Klasse entstehenden Glieder in 2 verschwindet, wenn $\pi > 5$, $\pi > 7$, ... respective ist.

Hieraus folgt für den Fall, wo π gerade ist, dass in II nur diejenigen Glieder übrig bleiben, welche dem Reste 0 entsprechen und die gleich 1 sind. Für diese aber ist $m = p^{\frac{1}{2}\pi}$, so dass die Summe aller Glieder in II gleich $p^{\frac{1}{2}\pi}$ wird.



Bemerkungen.

I. Zu Seite 589—601.

Artikel 237. Vgl. *Arithmetische Untersuchungen*, Artikel 61 u. 62, oben S. 41 u. 42.

Artikel 239. Vgl. *Arithmetische Untersuchungen*, Artikel 53, 55 u. 65, oben S. 35, 36 u. 44.

Artikel 241. Wenn $n = 2^\nu$ und $\nu \geqq 3$ so existiert zwar keine Zahl ρ von der angegebenen Art, aber die ganze Untersuchung wird hierdurch nicht wesentlich geändert.

Artikel 251. Vermutlich sollte die hier bemerkte Schwierigkeit durch die Einführung höherer Potenzen von p als Moduln beseitigt werden. Vgl. Artikel 363 S. 621, 372 S. 626, 373 S. 627.

II. Zu Seite 602—629.

Artikel 338. Wegen der Anspielung auf einen versprochenen Beweis des im ersten Abschnitt dieses Artikels enthaltenen Satzes kann man Artikel 44 der *Arithmetischen Untersuchungen* oben S. 29, vergleichen.

Artikel 348. Bei der Behauptung, dass die Coefficienten A', B', ... des entwickelten Products ganze rationale Zahlen sind, wird auf das sechste Kapitel verwiesen, in welchem aber die Theorie der Gleichung $x^\tau - 1 = 0$ nur für den Fall behandelt wird, dass τ eine Primzahl ist; die Form des Beweises im Artikel 349 führt zunächst auf folgende Ergänzung. Wird das entwickelte Product in die (für alle Wurzeln der Gleichung $\vartheta^\tau = 1$ geltende) Form

$$S = E + F\vartheta + \cdots + N\vartheta^{\tau-1}$$

gebracht, so sind die Coefficienten $E, F, \ldots, N$ ganze rationale Functionen von x mit ganzen rationalen Coefficienten; da ferner das Product ungeändert bleibt, wenn ϑ durch ϑ^k ersetzt wird, wo k irgend eine zu τ prime Zahl bedeutet, so gilt dasselbe von dem Ausdruck S, und hieraus ergiebt sich ohne Schwierigkeit, dass alle diejenigen in S enthaltenen Potenzen von ϑ, deren Exponenten s einen und denselben grössten gemeinschaftlichen Teiler mit τ haben, auch identische Coefficienten haben müssen; da endlich eine jede Summe solcher Potenzen ϑ^s immer eine ganze Zahl ist, so leuchtet ein, dass der Ausdruck S, und folglich auch das in Rede stehende Product eine ganze Function von x mit ganzen Coefficienten ist, was zu zeigen war. Ebenso geht aus dieser Betrachtung zugleich die Richtigkeit der Bemerkung am Schlusse des Paragraphen hervor. Andere Gründe lassen indessen vermuten, dass dem Verfasser schon damals das allgemeine Theorem über die Transformation der symmetrischen Functionen (*Demonstratio nova altera theorematis omnem functionem etc.*, Artikel 4) bekannt war, aus welchem sich die obigen Sätze als unmittelbare Folgerungen ergeben.

Artikel 352. Das Zeichen $R \equiv S$ (mod. P) oder auch $R \equiv S$ (mod. P, p) bedeutet hier und im Folgenden, dass die Differenz $R - S$ nach dem Modul p den Teiler P hat. — Das unvollständige Citat kann auf *Arithm. Unters.* Artikel 49 bezogen werden.

Artikel 354. Durch Multiplikation mit $x^\nu - 1$ ergiebt sich, dass die Summen gleich hoher Potenzen der Wurzeln der beiden Gleichungen $(P, \rho^{k\nu+t}) = 0$, $(P, \rho^t) = 0$ einander congruent sind (mod. p) und hieraus folgt die Congruenz $(P, \rho^{k\nu+t}) \equiv (P, \rho^t)$ (mod. p), sobald $m < p$ ist (vgl. Artikel 244); ist aber $m \geqq p$, so lässt sich der Coefficient der Potenz x^{m-p} in einer Gleichung nicht mehr aus den gegebenen Potenzsummen ihrer Wurzeln nach dem Modul p bestimmen, weil er in den hierzu dienenden Newton'schen Formeln mit dem Factor p behaftet ist. In der That darf man aus der Congruenz je zweier gleich hoher Potenzsummen der Wurzeln der Gleichungen $A = 0$, $B = 0$ allgemein nur folgern, dass $A \equiv \mathfrak{A}^p \mathfrak{C}$, $B \equiv \mathfrak{B}^p \mathfrak{C}$ (mod. p) ist, wo $\mathfrak{C}$ den grössten gemeinschaftlichen Teiler der beiden Functionen A, B nach dem Primzahl-Modulus p bezeichnet, $\mathfrak{A}$, $\mathfrak{B}$ aber ganz unbestimmte Functionen sind. Es ist zu vermuten, dass der Verfasser die Allgemeingültigkeit des Satzes aus der Theorie der Transformation der symmetrischen Functionen und speciell aus dem folgenden Satze abgeleitet hat: Ist in Bezug auf einen beliebigen Modulus p die Differenz $R(x) - S(x)$ teilbar durch die Function $P(x)$, und sind $a, b, c, \ldots$ die Wurzeln der Gleichung $P(x) = 0$, so sind die Functionen

$$(x - R(a))\,(x - R(b))\,(x - R(c)) \ldots \text{ und } (x - S(a))\,(x - S(b))\,(x - S(c)) \ldots$$

einander nach dem Modul p congruent.

Artikel 355. Es wird im Artikel 368 gezeigt, dass P und $\frac{dP}{dx}$ keinen gemeinschaftlichen Teiler haben, wenn P keinen Factor mehr als einmal enthält.

Artikel 361. Hier bedeutet der Exponent $\frac{1}{k}$ in dem Zeichen $(\xi, \rho^{\frac{1}{k}})$ jede ganze positive Zahl k' von der Beschaffenheit, dass $kk' \equiv 1$ (mod. ν) wird, wo ν die kleinste positive ganze Zahl ist, für welche $x^\nu - 1$ durch ξ nach dem Modul p teilbar wird; hierbei ist vorauszusetzen, dass ξ nicht durch x teilbar nach dem Modul p, und ausserdem, dass k relative Primzahl zu ν ist. Die Richtigkeit der Behauptung, dass ξ' durch $(\xi, \rho^{\frac{1}{k}})$ teilbar ist (mod. p), ergiebt sich aus Artikel 354.

Artikel 363. Die Schlussbemerkung bezieht sich vermutlich auf die Einführung von Moduln, welche Potenzen der Primzahl p sind; vgl. Artikel 251, 372, 373.

Artikel 367. Die Wurzeln der Gleichung $x^3 + x^2 - 2x - 1 = 0$ sind die zweigliedrigen Perioden, in welche die Wurzeln der Gleichung $\frac{x^7 - 1}{x - 1} = 0$ zerfallen.

Artikel 372. Wegen des unvollständigen Citats vgl. Artikel 251, 363.

III. Zu Seite 653. 654.

Dieses Fragment bezieht sich auf „*Arithmetische Untersuchungen*," Artikel 306, IX.

IV. Zu Seite 655—677.

a) Zu I und II.

Die zweite Formel für die Anzahl der innerhalb des Kreises liegenden Punkte (I. Artikel 3 und II. Artikel 5) ergiebt sich aus der Betrachtung des in denselben

eingeschriebenen Quadrats, dessen Seiten den Coordinatenachsen parallel sind; die Vergleichung beider Formeln führt zu dem auch arithmetisch leicht zu beweisenden Satze:

$$r' + r'' + \cdots + r^{(q)} = q^2 + r^{(q+1)} + r^{(q+2)} + \cdots + r^{(r)},$$

aus welchem sich wieder die Richtigkeit der ersten von den folgenden beiden Regeln ergiebt, die sich auf einem besonderen Blatt vorfanden:

„Auflösungen der Gleichung $x^2 + y^2 \leqq A$; Formel:

$$1 + 4\sqrt{A} + 4\sqrt{\tfrac{1}{2}A} + 8\,\Sigma\,(\sqrt{A-n^2} - n),$$

wo bei jeder Wurzel der Bruch weggelassen und von $n = 1$ bis $n = \sqrt{A}$ „(soll heissen $\sqrt{\tfrac{1}{2}A}$)“ summiert wird.

Andere Formel:

$$1 + 4\left\{A - \frac{A}{3} + \frac{A}{5} - \frac{A}{7} + \frac{A}{9} - \frac{A}{11} + \cdots\right\},$$

wo bei jedem Teil der Bruch weggelassen.“

Diese letztere Formel folgt aus dem später (I. Artikel 6) zur Anwendung kommenden Satze über die Anzahl der verschiedenen Darstellungen einer bestimmten Zahl durch die Form $x^2 + y^2$ (vgl. *Arithm. Unters.* Artikel 182 Anmerk., oben S. 150), welcher leicht in den folgenden umgeformt werden kann: Die Anzahl der verschiedenen Darstellungen einer positiven ganzen Zahl m durch die Form $x^2 + y^2$ ist gleich $4(a - b)$, wo a, b die Anzahlen der Teiler von m bedeuten, welche respective von der Form $4n + 1$, $4n + 3$ sind. Aus der Vergleichung dieser arithmetischen Formel mit der (in I Artikel 5 oder II Artikel 4) durch geometrische Betrachtungen gewonnenen mittleren Darstellungsanzahl erhält man leicht und in aller Strenge das bekannte Resultat

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots,$$

welches in der Abhandlung durch eine ähnliche Vergleichuug, aber mit Hülfe unendlicher Producte abgeleitet wird.

b) Zu III und IV.

Ist C der Complex aller positiven nicht eigentlich äquivalenten eigentlich primitiven Formen von negativer Determinante $-D$, und legt man den Variabeln dieser Formen je zwei Werte bei, welche relative Primzahlen zu einander sind, so ist die Anzahl aller Darstellungen einer positiven ganzen Zahl m gleich $\varepsilon\psi(m)$, wo ε die Anzahl der Auflösungen der Gleichung $t^2 + Du^2 = 1$ und $\psi(m)$ die Anzahl derjenigen Wurzeln der Congruenz $n^2 + D \equiv 0 \pmod{m}$ bedeutet, für welche die drei Zahlen m, $2n$ und $\frac{n^2+D}{m}$ ohne gemeinschaftlichen Teiler sind (*Arithm. Unters.* Artikel 180, vgl. oben S. 147). Der Factor ε ist $= 4$ für $D = 1$, in allen anderen Fällen $= 2$. Ist ferner $m = p^\pi p'^{\pi'} p''^{\pi''} \ldots$, wo p', p'', p''' ... von einander verschiedene Primzahlen bedeuten, so ist $\psi(m) = \psi(p^\pi)\psi(p'^{\pi'})\psi(p''^{\pi''})\ldots$; bedeutet $\mathfrak{A}(m)$ die Anzahl der Wurzeln der Congruenz $n^2 + D \equiv 0 \pmod{m}$, und bedient man sich des von Legendre eingeführten, von Jacobi verallgemeinerten Zeichens, so ist $\psi(p^\pi) = \mathfrak{A}(p^\pi) = 1 + \left(\frac{-D}{p}\right)$

wenn p nicht in $2D$ aufgeht, sonst aber $= \mathfrak{A}(p^\pi) - \frac{1}{p}\mathfrak{A}(p^{\pi+1})$; die Anzahl $\mathfrak{A}(p^\pi)$ lässt sich immer leicht bestimmen (*Arithm. Unters.* Artikel 104, vgl. oben S. 72), für die Folge reicht aber die Bemerkung aus, dass $\mathfrak{A}(p^\pi)$ immer von π unabhängig wird, sobald π eine gewisse Grösse überschreitet.

Legt man den Variabeln der in dem Complex C enthaltenen Formen alle ganzzahligen Werte ohne Ausnahme bei (*Arithm. Unters.* Artikel 181, vgl. oben S. 148), so wird die Anzahl (m) aller Darstellungen der Zahl m gleich $\varepsilon f(m)$, wo $f(m) = \Sigma\psi\left(\frac{m}{\mu^2}\right)$ ist, und das Summenzeichen sich auf alle quadratischen Teiler μ^2 der Zahl m bezieht. Hieraus folgt unmittelbar:

$$f(m) = f(p^\pi p'^{\pi'} p''^{\pi''} \ldots) = f(p^\pi) f(p'^{\pi'}) f(p''^{\pi''}) \ldots$$

und

$$f(p^\pi) = \psi(p^\pi) + \psi(p^{\pi-2}) + \psi(p^{\pi-4}) + \cdots,$$

welche Reihe so lange fortzusetzen ist, als die Exponenten π, $\pi - 2$, $\pi - 4$, ... nicht negativ werden. Wenn p nicht in $2D$ aufgeht, so folgt hieraus:

$$f(p^\pi) = 1 + \left(\frac{-D}{p}\right) + \left(\frac{-D}{p^2}\right) + \cdots + \left(\frac{-D}{p^\pi}\right),$$

und allgemein, wenn m relative Primzahl zu $2D$ ist:

$$f(m) = \Sigma\left(\frac{-D}{n}\right),$$

wo das Summenzeichen sich auf alle Teiler n der Zahl m bezieht.

Aus diesen Bemerkungen ergiebt sich unmittelbar die Richtigkeit der im Text (III, 1, 2, 3) aufgestellten Sätze über die Anzahl (m), wenn man für den ersten derselben noch die Bedingung hinzufügt, dass D nicht durch p^2 teilbar sein darf (die Bestimmung der Klassenanzahl ist schon in den „*Arithmetischen Untersuchungen*" Artikel 256 auf den Fall zurückgeführt, in welchem D durch kein Quadrat teilbar ist). Zugleich findet man, auch ohne Rücksicht auf diese Beschränkung, dass die unendliche Reihe

$$1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \frac{f(p^3)}{p^3} + \cdots$$

den Wert

$$\frac{1}{1-\frac{1}{p}} \quad \text{oder} \quad \frac{1}{1-\frac{1}{p}} \cdot \frac{1}{1-\left(\frac{-D}{p}\right)\cdot\frac{1}{p}}$$

hat, je nachdem $2D$ durch die Primzahl p teilbar oder nicht teilbar ist.

c) Zu V.

Die zu Formel III hinzugefügte Bemerkung giebt den Weg an, auf welchem der Verfasser zur Bestimmung der Anzahl k der in dem Complex C enthaltenen Formen gelangt ist. Aus geometrischen Betrachtungen (vgl. I Artikel 5 und II Artikel 4) ergiebt sich, dass der Grenzwert, welchem sich der Quotient

$$\frac{(1) + (2) + (3) + \cdots + (m)}{m}$$

mit unbegrenzt wachsendem m nähert, d. h. die mittlere Anzahl der Darstellungen einer unbestimmten positiven ganzen Zahl

$$= k \frac{\pi}{\sqrt{D}}$$

ist; ein zweiter Ausdruck für denselben Grenzwert lässt sich auf verschiedene Arten aus der Natur der im Vorhergehenden bestimmten Anzahl $(m) = \varepsilon f(m)$ der Darstellungen der Zahl m ableiten. Der zu diesem Zweck von dem Verfasser zunächst eingeschlagene Weg scheint nach den vorhandenen Bruchstücken (I Artikel 7 und 8; III und IV) folgender gewesen zu sein.

Ist $\vartheta(m)$ irgend eine Function der positiven ganzen Zahl m, und p irgend eine Primzahl, so kann man aus $\vartheta(m)$ immer eine neue Function $\vartheta'(m)$ ableiten, deren Wert unabhängig davon ist, ob und wie oft p als Factor in m enthalten ist, und welche für alle durch p nicht teilbaren Zahlen m mit $\vartheta(m)$ übereinstimmt; eine solche Function erhält man, wenn man $\vartheta'(m) = \vartheta\left(\frac{m}{p^\pi}\right)$ setzt, wo p^π die höchste in m aufgehende Potenz von p bedeutet; und man kann sagen, dass die Function $\vartheta'(m)$ aus $\vartheta(m)$ durch Elimination der Primzahl p entsteht. Bildet man auf diese Weise aus $f(m)$ eine neue Function $f'(m)$ durch Elimination der Primzahl 2, aus dieser die Function $f''(m)$ durch Elimination von 3 u. s. f., so wird jede folgende dieser Functionen einen regelmässigeren Verlauf haben, als die vorhergehenden; eliminiert man eine Primzahl nach der anderen, wie sie ihrer Grösse nach auf einander folgen, so wird eine solche Function $\vartheta(m)$ für unendlich viele Werte von m den Wert $f(1) = 1$ haben und namentlich für alle diejenigen Werte von m, welche kleiner sind als die zuletzt eliminierte Primzahl. Durch unendliche Fortsetzung dieses Processes nähert man sich immer mehr der Function $f^\infty(m)$, welche für alle Werte von m den Wert 1 hat, und deren mittlerer Wert folglich ebenfalls gleich 1 ist. Gelingt es nun, den mittleren Wert irgend einer Function $\vartheta(m)$ durch denjenigen der nächstfolgenden $\vartheta'(m)$ auszudrücken, so wird man auch den mittleren Wert der Function $f(m)$ durch eine unendliche Kette von Operationen finden können.

Ist p die Primzahl, durch deren Elimination $\vartheta'(m)$ aus $\vartheta(m)$ entsteht, so ist $\vartheta(m) = \vartheta'(m) f(p^\pi)$, wenn p^π wieder die höchste in m aufgehende Potenz von p bedeutet. Für diesen Fall, dass p nicht in $2D$ aufgeht, findet man leicht, dass

$$\vartheta'(m) = \vartheta(mp) - \left(\frac{-D}{p}\right) \vartheta(m)$$

ist; setzt man zur Abkürzung:

$$\Theta(m) = \vartheta(1) + \vartheta(2) + \cdots + \vartheta(m)$$
$$\Theta'(m) = \vartheta'(1) + \vartheta'(2) + \cdots + \vartheta'(m),$$

so ergiebt sich:

$$\Theta'(mp) = \Theta(mp) - \left(\frac{-D}{p}\right) \Theta(m)$$

und hieraus, wenn man mit ω, ω' respective die mittleren Werte der Functionen $\vartheta(m)$, $\vartheta'(m)$ bezeichnet:

$$\omega = \frac{\omega'}{1 - \left(\frac{-D}{p}\right)\frac{1}{p}}.$$

Wenn aber die Primzahl p in $2D$ aufgeht, so findet zwar zwischen den Functionen $\vartheta(m)$ und $\vartheta'(m)$ im Allgemeinen keine so einfache Beziehung mehr statt; indessen ergiebt sich auf ähnliche Art leicht, dass in diesem Falle $\omega = \omega'$ wird. Ein anderer Weg, die Beziehung zwischen ω und ω' in beiden Fällen abzuleiten, ist folgender. Setzt man

$$\delta(m) = \Sigma\vartheta(\mu),$$

wo das Summenzeichen sich auf alle Zahlen μ bezieht, die nicht durch p teilbar und ausserdem nicht grösser als m sind, und bezeichnet man mit m', m'', m''', ... resp. die grössten in $\frac{m}{p}, \frac{m'}{p}, \frac{m''}{p}, \cdots$ enthaltenen ganzen Zahlen, so ist

$$\Theta(m) = \delta(m) + \delta(m')f(p) + \delta(m'')f(p^2) + \delta(m''')f(p^3) + \cdots$$
$$\Theta'(m) = \delta(m) + \delta(m') + \delta(m'') + \delta(m''') + \cdots$$

und hieraus folgt:

$$\frac{\omega}{\omega'} = \left(1 - \frac{1}{p}\right)\left\{1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \frac{f(p^3)}{p^3} + \cdots\right\},$$

was mit dem oben gefundenen Resultat übereinstimmt (vgl. die Note zu III und IV).

Der mittlere Wert der Function $f(m)$ ist daher gleich dem unendlichen Product

$$\prod \frac{1}{1 - \left(\frac{-D}{p}\right)\frac{1}{p}},$$

in welchem p alle in $2D$ nicht aufgehenden Primzahlen durchlaufen muss, und hieraus folgt:

$$k = \frac{\varepsilon\sqrt{D}}{\pi}\prod \frac{1}{1 - \left(\frac{-D}{p}\right)\frac{1}{p}}.$$

Hinsichtlich der Strenge dieser Deduction bleibt aber ein Bedenken übrig, welches sich auf die Methode bezieht, den mittleren Wert der Function $f(m)$ durch successive Elimination aller Primzahlen zu bestimmen; denn wenn es auch einleuchtet, dass der Wert der durch Elimination der ersten n Primzahlen erhaltenen Function $f^{(n)}(m)$ mit dem der Function $f^{\infty}(m) = 1$ übereinstimmt, so lange m kleiner bleibt als die zuletzt eliminierte Primzahl, und dass also durch die Wahl eines hinreichend grossen Wertes n diese Übereinstimmung bis zu jeder vorher vorgeschriebenen Grösse der Zahl m getrieben werden kann, so ist hiermit allein doch keineswegs erwiesen, dass mit unbegrenzt wachsendem n der mittlere Wert der Function $f^{(n)}(m)$ sich dem mittleren Werte der Function $f^{\infty}(m)$, d. h. dem Werte 1 unbegrenzt nähert. In welcher Weise der Verfasser diese Lücke auszufüllen gedachte, lässt sich aus den vorhandenen Papieren nicht mit Sicherheit bestimmen; doch führt die schon oben (in der Note zu I) mitgeteilte Formel

$$1 + 4\left\{A - \frac{A}{3} + \frac{A}{5} - \frac{A}{7} + \frac{A}{9} - \frac{A}{11} + \cdots\right\}$$

für die Anzahl der Paare von Zahlen, deren Quadratsumme den Wert A nicht über-

trifft, zu der Vermutung, dass der Verfasser mit Umgehung des unendlichen Products, für den mittleren Wert der Function $f(m)$ unmittelbar die unendliche Reihe

$$\sum \left(\frac{-D}{n}\right)\frac{1}{n}$$

gefunden habe, in welcher n der Grösse nach alle positiven ganzen Zahlen durchlaufen muss, die relative Primzahlen zu $2D$ sind. Die einfachste Art, diesen Uebergang anzudeuten, scheint die folgende zu sein.

Ist μ der grösste aller derjenigen Teiler einer Zahl m, welche relative Primzahlen zu $2D$ sind, und setzt man $\vartheta(m) = f(\mu)$, so ist $\vartheta(m)$ diejenige Function, welche durch Elimination aller in $2D$ aufgehenden Primzahlen aus $f(m)$ entsteht, und deren mittlerer Wert nach dem Obigen mit demjenigen der Function $f(m)$ übereinstimmt. Da nun $\vartheta(m) = \Sigma\left(\frac{-D}{n}\right)$ ist, wo n alle Teiler von μ, d. h. alle diejenigen Teiler von m durchläuft, welche relative Primzahlen zu $2D$ sind, so ergiebt sich die der obigen analoge Formel

$$\Theta(m) = \vartheta(1) + \vartheta(2) + \cdots + \vartheta(m) = \sum \left(\frac{-D}{n}\right)\frac{m}{n},$$

wo in der Summe rechter Hand der Buchstabe n alle relativen Primzahlen zu $2D$ durchläuft, und von den Quotienten $\frac{m}{n}$ immer nur die grösste in ihm enthaltene ganze Zahl beizubehalten ist. Ordnet man die Glieder dieser Reihe so, dass die Zahlen n ihrer Grösse nach auf einander folgen, so nimmt der Factor $\frac{m}{n}$ fortwährend ab oder doch wenigstens nie zu, und die Reihe bricht ab, sobald $n > m$ wird. Ausserdem ergiebt sich aus dem Fundamentaltheorem in der Theorie der quadratischen Reste und aus der Verallgemeinerung desselben, dass die Summe von je $\varphi(4D)$ auf einander folgenden Werten des Factors $\left(\frac{-D}{n}\right)$ verschwindet, woraus folgt, dass die Summe von noch so vielen auf einander folgenden Werten desselben ihrem absoluten Wert nach die endliche nur von der Determinante D abhängige Grösse $\Delta = \varphi(2D)$ niemals übertrifft. Verbindet man diese beiden Bemerkungen mit einander, so findet man leicht, dass die Summe aller auf das Glied $\left(\frac{-D}{n}\right)\frac{m}{n}$ folgenden Glieder absolut genommen kleiner als $\Delta\frac{m}{n}$ ist, und dass folglich der Quotient $\Theta(m) : m$ bei unendlich wachsendem m die in der angegebenen Art geordnete, convergierende unendliche Reihe

$$\sum \left(\frac{-D}{n}\right)\frac{1}{n}$$

zum Grenzwerte hat. Nachdem so der gemeinschaftliche mittlere Wert der Functionen $\vartheta(m)$ und $f(m)$ gefunden ist, erhält man unmittelbar:

$$k = \frac{\varepsilon\sqrt{D}}{\pi}\sum \left(\frac{-D}{n}\right)\frac{1}{n}.$$

Es verdient noch bemerkt zu werden, dass die Artikel 6 und 8 der Abhandlung II auf eine in mancher Beziehung einfachere und auch leicht auszuführende Behandlungsweise des Problems hindeuten, bei welcher nur die Darstellungen ungerader oder sogar nur solcher Zahlen betrachtet werden, die relative Primzahlen zu $2D$ sind.

d) Zu VI und VII.

Die Art, wie der Verfasser die Summation der Reihe $\sum\left(\frac{-D}{n}\right)\frac{1}{n}$ ausgeführt hat, ergiebt sich aus einigen speciellen Beispielen, welche sich auf einzelnen Blättern vorfinden.

Ist $D \equiv 3 \pmod{4}$, so folgt aus dem Fundamentaltheorem in der Theorie der quadratischen Reste mit Benutzung der Reihe

$$\operatorname{cotang} u = \frac{1}{u} + \frac{1}{u-\pi} + \frac{1}{u+\pi} + \frac{1}{u-2\pi} + \frac{1}{u+2\pi} + \cdots,$$

dass

$$\sum\left(\frac{-D}{n}\right)\frac{1}{n} = \sum\left(\frac{n}{D}\right)\frac{1}{n} = \frac{\pi}{2D}\sum\left(\frac{\nu}{D}\right)\operatorname{cotang}\frac{\nu\pi}{2D}$$

ist, wo ν alle relativen Primzahlen zu $2D$ durchläuft, die kleiner als D sind; setzt man

$$\sqrt{-1} = i, \quad \cos\frac{2\pi}{D} + i\sin\frac{2\pi}{D} = r$$

und bezeichnet man mit μ alle relativen Primzahlen zu D, welche nicht grösser als D sind, so lässt die vorstehende Summe sich leicht in die folgende umformen:

$$\sum\left(\frac{-D}{n}\right)\frac{1}{n} = \frac{\pi i}{4D}\left(\frac{2}{D}\right)\sum\left(\frac{\mu}{D}\right)\frac{r^{\mu}-1}{r^{\mu}+1};$$

wendet man nun die für jede Wurzel ω der Gleichung $\omega^D = 1$ gültige Formel

$$\frac{\omega-1}{\omega+1} = \sum(-1)^{\alpha-1}\,\omega^{\alpha},$$

in welcher α die Zahlen $1, 2, 3, \ldots, D-1$ durchlaufen muss, an, so erhält man durch Umkehrung der Summationsordnung

$$\sum\left(\frac{-D}{n}\right)\frac{1}{n} = \frac{\pi i}{4D}\left(\frac{2}{D}\right)\sum(-1)^{\alpha-1}\sum\left(\frac{\mu}{D}\right)r^{\alpha\mu}.$$

Die auf μ bezügliche Summation lässt sich bekanntlich mit Hülfe der in der Abhandlung: „*Summierung gewisser Reihen von besonderer Art*“ (vgl. oben S. 463) bewiesenen Sätze ausführen; beschränkt man sich auf den Fall, in welchem D durch kein Quadrat teilbar ist, so findet man allgemein:

$$\sum\left(\frac{\mu}{D}\right)r^{\alpha\mu} = \left(\frac{\alpha}{D}\right)i^{\left(\frac{D-1}{2}\right)^2}\sqrt{D},$$

wo $\left(\frac{\alpha}{D}\right) = 0$ gesetzt werden muss, falls α keine relative Primzahl zu D ist. In dem Fall $D \equiv 3 \pmod{4}$ erhält man daher:

$$\sum\left(\frac{-D}{n}\right)\frac{1}{n} = \frac{\pi}{4\sqrt{D}}\left(\frac{2}{D}\right)\sum\left(-1\right)^{\alpha}\left(\frac{\alpha}{D}\right) = \frac{\pi}{2\sqrt{D}}\sum\left(\frac{\alpha'}{D}\right),$$

wo α' alle relativen Primzahlen zu D durchläuft, die kleiner als $\frac{1}{2}D$ sind; da endlich $\varepsilon = 2$ ist, so wird die Anzahl der Klassen

$$k = \sum\left(\frac{\alpha'}{D}\right).$$

Ist dagegen $D \equiv 1 \pmod{4}$, so erhält man mit Benutzung der Reihe

$$\operatorname{cosec} u = \frac{1}{u} - \frac{1}{u-\pi} - \frac{1}{u+\pi} + \frac{1}{u-2\pi} + \frac{1}{u+2\pi} - \cdots$$

auf ähnliche Weise

$$\sum \left(\frac{-D}{n}\right)\frac{1}{n} = \sum (-1)^{\frac{n-1}{2}} \left(\frac{n}{D}\right)\frac{1}{n}$$

$$= \frac{\pi}{2D} \sum (-1)^{\frac{\nu-1}{2}} \left(\frac{\nu}{D}\right) \operatorname{cosec} \frac{\nu\pi}{2D}$$

$$= \frac{\pi}{2D} \sum \left(\frac{\mu}{D}\right) \frac{r^{\mu}}{r^{2\mu}+1},$$

wo die Buchstaben ν und μ die frühere Bedeutung haben; schliesst man den evidenten Fall $D=1$ aus und wendet die für jede Wurzel ω der Gleichung $\omega^D = 1$ (mit Ausnahme von $\omega = 1$) gültige Formel

$$\frac{\omega}{\omega^2+1} = 1 + \sum \omega^{4\alpha''} + \sum \omega^{D-4\alpha''},$$

in welcher α'' die Zahlen $1, 2, 3, \ldots, \frac{1}{4}(D-1)$ durchlaufen muss, an, so ergiebt sich, wieder unter der Beschränkung, dass D durch kein Quadrat teilbar ist:

$$\sum \left(\frac{-D}{n}\right)\frac{1}{n} = \frac{\pi}{\sqrt{D}} \sum \left(\frac{\alpha''}{D}\right)$$

und hieraus, da $\varepsilon = 2$ ist:

$$k = 2\sum \left(\frac{\alpha''}{D}\right).$$

Ganz ähnlich würden sich die Fälle behandeln lassen, in welchen D gerade ist. —

Was die Bestimmung der Klassenanzahl für positive Determinanten D betrifft, so finden sich ausser der im Text mitgeteilten Schlussformel nur einzelne geometrische Figuren vor, welche Hyperbelsectoren von endlichen Dimensionen darstellen, und neben denselben Ungleichungen, durch welche die Punkte, deren Coordinaten die Variablen der quadratischen Formen sind, in das Innere eines solchen Hyperbelsectors gedrängt werden. Diese Hyperbelsectoren treten an die Stelle der Ellipsen, welche den quadratischen Formen mit negativer Determinante entsprechen, und durch die Bestimmung ihres Flächeninhalts ergiebt sich wieder die mittlere Darstellungsanzahl, wenn nämlich nur solche Darstellungen zugelassen werden, bei welchen die Variabeln den eben erwähnten Ungleichungen Genüge leisten. Andererseits dienen diese Ungleichungen dazu, aus den unendlich vielen Darstellungen einer Zahl m, welche alle zu einer und derselben Wurzel n der Congruenz $n^2 - D \equiv 0 \left(\operatorname{mod.} \frac{m}{\mu^2}\right)$ gehören und welche den sämtlichen Auflösungen der Gleichung $t^2 - Du^2 = 1$ entsprechen (vgl. *Arithmetische Untersuchungen* Artikel 205), eine einzige zu isolieren und alle andern auszuschliessen. Die Anzahl aller zugelassenen Darstellungen derZahl m durch den Complex aller nicht eigentlich äquivalenten eigentlich primitiven Formen ist dann gleich

dem Wert der Function $f(m)$, in welcher nur $-D$ durch D zu ersetzen ist, und aus der Betrachtung der Eigenschaften derselben ergiebt sich, wie früher bei negativen Determinanten, ein zweiter Ausdruck für die mittlere Darstellungsanzahl; die Vergleichung desselben mit dem vorher durch geometrische Betrachtungen abgeleiteten Werte führt dann unmittelbar zu der Bestimmung der Anzahl der Klassen.

e) Zu VIII.

Hier bedeutet p eine positive Primzahl von der Form $4n+1$; die Bezeichnung stimmt mit der in der Abhandlung: *Theorie der biquadratischen Reste* I Artikel 23 (vgl. oben S. 531) angewendeten überein; es ist also

$$f \equiv 1 \cdot 2 \cdot 3 \cdots \frac{1}{2}(p-3) \cdot \frac{1}{2}(p-1) \pmod{p}$$

$$p = a^2 + b^2; \quad a \equiv 1 \pmod{4}; \quad b \equiv af \pmod{p};$$

die mit α, β bezeichneten Zahlen sind durch die Zerlegung $p = \alpha^2 + 2\beta^2$ bestimmt.

Der im Text aufgestellte Satz hängt mit dem biquadratischen Character der Zahl 2 zusammen; da nämlich (vgl. *Theorie der biquadratischen Reste* I. Artikel 21, oben S. 529)

$$2^{\frac{p-1}{4}} \equiv f^{\frac{1}{2}b} \pmod{p}$$

ist, so folgt aus der Congruenz

$$b \equiv 2m + a - 1 \pmod{8}$$

die andere

$$2^{\frac{p-1}{4}} \equiv f^{m+\frac{a-1}{2}} \pmod{p}$$

und umgekehrt jene aus dieser. Der Beweis dieser letzteren Congruenz ergiebt sich leicht auf folgende Art. Ist μ die Anzahl der quadratischen Reste α_1, welche zwischen 0 und $\frac{1}{4}p$ liegen, so ist (nach VII):

$$m = 2\mu - \tfrac{1}{4}(p-1),$$

und die Anzahl der quadratischen Reste α_2, welche zwischen $\frac{1}{4}p$ und $\frac{1}{2}p$ liegen, ist $= \frac{1}{4}(p-1) - \mu$. Ist nun $p \equiv 1 \pmod{8}$, also die Zahl 2 quadratischer Rest, so stimmen die Zahlen $2\alpha_1$ und $p - 2\alpha_2$ im Complex mit den Zahlen α_1 und α_2 überein, und bezeichnet man das Product dieser Zahlen mit A, so ergiebt sich:

$$2^{\frac{p-1}{4}} A \equiv (-1)^{\frac{1}{4}(p-1)-\mu} A \pmod{p}.$$

und folglich:

$$2^{\frac{p-1}{4}} \equiv (-1)^{\mu} \equiv f^{2\mu} \equiv f^{m+\frac{1}{4}(p-1)} \pmod{p}.$$

Da ferner in diesem Fall $b \equiv 0 \pmod{4}$ und folglich

$$\frac{p-1}{4} = (a+1)\frac{a-1}{4} + \frac{b^2}{4} \equiv 2\frac{a-1}{4} \equiv \frac{a-1}{2} \pmod{4}$$

ist, so erhält man die zu beweisende Congruenz:

$$2^{\frac{p-1}{4}} \equiv f^{m+\frac{a-1}{2}} \pmod{p}.$$

Ist dagegen $p \equiv 5 \pmod{8}$, also die Zahl 2 quadratischer Nichtrest, so stimmen die Zahlen $2\alpha_1$ und $p - 2\alpha_2$ mit den sämtlichen zwischen 0 und $\frac{1}{2}p$ liegenden quadratischen Nichtresten überein; bezeichnet man ihr Product mit B und das Product der Zahlen α_1 und α_2 wieder mit A, so ist

$$f \equiv AB, \quad (-1)^{\frac{p-1}{4} - \mu} \cdot 2^{\frac{p-1}{4}} A \equiv B \pmod{p}.$$

Erhebt man diese beiden Congruenzen zum Quadrat, indem man berücksichtigt, dass

$$f^2 \equiv -1, \quad 2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

ist, so erhält man:

$$-1 \equiv A^2 B^2, \quad -A^2 \equiv B^2$$

und hieraus $A^4 \equiv +1$; da nun A ein Product aus quadratischen Resten, also A^2 ein Product aus biquadratischen Resten und folglich selbst ein biquadratischer Rest ist, so muss $A^2 \equiv +1$ sein, weil -1 ein biquadratischer Nichtrest ist. Hieraus folgt:

$$(-1)^{\frac{p-1}{4} - \mu}\, 2^{\frac{p-1}{4}} \equiv AB \equiv f \pmod{p}$$

und

$$2^{\frac{p-1}{4}} \equiv (-1)^{\mu - 1} f \equiv f^{2\mu - 1} \equiv f^{m + \frac{p-5}{4}} \pmod{p}.$$

Da endlich in diesem Fall $b \equiv 2 \pmod{4}$ und folglich

$$\frac{p-5}{4} = (a+1)\frac{a-1}{4} + \frac{b^2-4}{4} \equiv 2\,\frac{a-1}{4} \equiv \frac{a-1}{2} \pmod{4}$$

ist, so erhält man wieder die zu beweisende Congruenz:

$$2^{\frac{p-1}{4}} \equiv f^{m + \frac{a-1}{2}} \pmod{p}.$$

f) Zu IX.

Es sei p eine positive ungerade durch kein Quadrat teilbare Zahl und

$$S_r = \sum \left(\frac{s_r}{p}\right),$$

wo s_r alle relativen Primzahlen zu p durchlaufen muss, welche zwischen $(r-1)\frac{p}{8}$ und $r\frac{p}{8}$ liegen; bezeichnet man die Anzahlen der nicht eigentlich äquivalenten eigentlich primitiven Formen für die Determinanten $-p$ und $-2p$ respective mit C_1, und C_2, so ist (vgl. Dirichlet *Recherches sur diverses applications* etc. § 11 in Crelle's Journ. XXI.).

$$C_1 = 2(S_1 + S_2), \quad C_2 = 2(S_1 - S_4)$$

oder

$$C_1 = S_1 + S_2 + S_3 + S_4, \quad C_2 = 2(S_2 + S_3),$$

je nachdem $p \equiv 1$ oder $\equiv 3 \pmod{4}$ ist. Bedenkt man ferner, dass die Zahlen s_1 und s_2 im Complex mit den Zahlen $2s_1$ und $p - 2s_4$, und ebenso die Zahlen s_3 und s_4 im

Complex mit den Zahlen $2s_2$ und $p-2s_3$ übereinstimmen, und dass im Falle $p\equiv 1$ (mod. 4) die Summe $S_1+S_2+S_3+S_4=0$ ist, so ergeben sich in beiden Fällen noch zwei neue Relationen zwischen den vier Summen S_1, S_2, S_3, S_4, so dass jede derselben durch C_1 und C_2 ausgedrückt werden kann. Man erhält auf diese Weise: wenn $p\equiv 1$ (mod. 4) ist:

$$S_1=S_8=\tfrac{1}{4}\left(\frac{2}{p}\right)C_1+\tfrac{1}{4}C_2$$

$$S_2=S_7=\tfrac{1}{4}\left(2-\left(\frac{2}{p}\right)\right)C_1-\tfrac{1}{4}C_2$$

$$S_3=S_6=-\tfrac{1}{4}\left(2+\left(\frac{2}{p}\right)\right)C_1+\tfrac{1}{4}C_2$$

$$S_4=S_5=\tfrac{1}{4}\left(\frac{2}{p}\right)C_1-\tfrac{1}{4}C_2,$$

und wenn $p\equiv 3$ (mod. 4) ist:

$$S_1=-S_8=\tfrac{1}{4}\left(3+\left(\frac{2}{p}\right)\right)C_1-\tfrac{1}{4}C_2$$

$$S_2=-S_7=-\tfrac{1}{4}\left(1-\left(\frac{2}{p}\right)\right)C_1+\tfrac{1}{4}C_2$$

$$S_3=-S_6=\tfrac{1}{4}\left(1-\left(\frac{2}{p}\right)\right)C_1+\tfrac{1}{4}C_2$$

$$S_4=-S_5=\tfrac{1}{4}\left(1-\left(\frac{2}{p}\right)\right)C_1-\tfrac{1}{4}C_2.$$

Ist p eine Primzahl, so findet man hieraus unmittelbar die im Texte angegebenen Formeln für die Anzahl der quadratischen Reste, welche in den einzelnen Octanten enthalten sind.

g) Zu X.

Es sei p eine positive und durch kein Quadrat teilbare Zahl von der Form $6n\pm 1$ und

$$S_r=\sum\left(\frac{s_r}{p}\right),$$

wo s_r alle relativen Primzahlen zu p durchlaufen muss, welche zwischen $(r-1)\frac{p}{12}$ und $r\frac{p}{12}$ liegen; bezeichnet man die Anzahlen der nicht eigentlich äquivalenten eigentlich primitiven Formen für die Determinanten $-p$ und $-3p$ mit C_1, C_3, so findet man leicht (vgl. Dirichlet, *Recherches* etc. § 11 oder die Note zu VI und VII):

$$C_1=2(S_1+S_2+S_3),\quad C_3=2(S_1+S_2-S_5-S_6)$$

oder:

$$C_1=S_1+S_2+S_3+S_4+S_5+S_6,\quad C_3=2(S_2+S_3+S_4+S_5),$$

je nachdem $p\equiv 1$ oder $\equiv 3$ (mod. 4) ist. Berücksichtigt man ferner, dass

die Zahlen s_1 und s_2 mit den Zahlen $2s_1$ und $p-2s_6$
„ „ s_3 und s_4 „ „ „ $2s_2$ und $p-2s_5$
„ „ s_5 und s_6 „ „ „ $2s_3$ und $p-2s_4$

und ebenso

die Zahlen s_1, s_2, s_3 mit den Zahlen $3s_1, 3s_5-p, p-3s_4$
„ „ s_4, s_5, s_6 „ „ „ $3s_2, 3s_6-p, p-3s_3$

übereinstimmen und dass im Falle $p\equiv 1 \pmod 4$ die Summe $S_1+S_2+S_3+S_4+S_5+S_6=0$ ist, so erhält man ausser den beiden obigen noch vier neue Relationen zwischen den sechs Summen $S_1, S_2, \ldots, S_6$, so dass dieselben sämtlich aus C_1 und C_3 bestimmt werden können. Man erhält auf diese Weise,

wenn $p\equiv 1 \pmod 4$ ist:

$$S_1=S_{12}=\tfrac{1}{4}\left(1+\left(\frac{3}{p}\right)\right)C_1+\tfrac{1}{12}\left(1+\left(\frac{2}{p}\right)\right)C_3$$

$$S_2=S_{11}=-\tfrac{1}{4}\left(1+\left(\frac{3}{p}\right)\right)C_1+\tfrac{1}{12}\left(1+\left(\frac{2}{p}\right)\right)C_3$$

$$S_3=S_{10}=\tfrac{1}{2}C_1-\tfrac{1}{6}\left(1+\left(\frac{2}{p}\right)\right)C_3$$

$$S_4=S_9=-\tfrac{1}{2}C_1-\tfrac{1}{6}\left(2-\left(\frac{2}{p}\right)\right)C_3$$

$$S_5=S_8=\tfrac{1}{4}\left(1+\left(\frac{3}{p}\right)\right)C_1-\tfrac{1}{12}\left(5-\left(\frac{2}{p}\right)\right)C_3$$

$$S_6=S_7=-\tfrac{1}{4}\left(1+\left(\frac{3}{p}\right)\right)C_1+\tfrac{1}{12}\left(1+\left(\frac{2}{p}\right)\right)C_3,$$

und wenn $p\equiv 3 \pmod 4$ ist:

$$S_1=-S_{12}=\tfrac{1}{12}\left(9+3\left(\frac{2}{p}\right)-\left(\frac{3}{p}\right)+\left(\frac{6}{p}\right)\right)C_1-\tfrac{1}{4}C_3$$

$$S_2=-S_{11}=\tfrac{1}{4}\left(-1+\left(\frac{2}{p}\right)+\left(\frac{3}{p}\right)-\left(\frac{6}{p}\right)\right)C_1+\tfrac{1}{4}C_3$$

$$S_3=-S_{10}=\tfrac{1}{6}\left(-\left(\frac{3}{p}\right)+\left(\frac{6}{p}\right)\right)C_1$$

$$S_4=-S_9=\tfrac{1}{6}\left(3-2\left(\frac{3}{p}\right)-\left(\frac{6}{p}\right)\right)C_1$$

$$S_5=-S_8=\tfrac{1}{4}\left(-1-\left(\frac{2}{p}\right)+\left(\frac{3}{p}\right)+\left(\frac{6}{p}\right)\right)C_1+\tfrac{1}{4}C_3$$

$$S_6=-S_7=\tfrac{1}{12}\left(3-3\left(\frac{2}{p}\right)+\left(\frac{3}{p}\right)-\left(\frac{6}{p}\right)\right)C_1-\tfrac{1}{4}C_3\,.$$

Ist p eine Primzahl, so findet man aus dem ersten System die im Texte angegebenen Formeln; für die andern Fälle erhält man ähnliche Formeln aus dem zweiten System.



Druck von G. Bernstein in Berlin.





